Secure Steganography for Digital Images

Meandering in the Dark

Khan Farhan Rafat
NUST, Rawalpindi/Islamabad
Pakistan

Muhammad Junaid Hussain
NUST, Rawalpindi/Islamabad
Pakistan

***Abstract*—The degree of imperceptibility of hidden image in the 'Digital Image Steganography' is mostly defined in relation to the limitation of Human Visual System (HVS), its chances of detection using statistical methods and its capacity to hide maximum information inside its body. Whereas, a tradeoff does exist between data hiding capacity of the cover image and robustness of underlying information hiding scheme. This paper is an exertion to underline the technique to embed information inside the cover at Stego key dependent locations, which are hard to detect, to achieve optimal security. Hence, it is secure under worst case scenario where Wendy is in possession of the original image (cover) agreed upon by Alice and Bob for their secret communication. Reliability of our proposed solution can be appreciated by observing the differences between cover, preprocessed cover and Stego object. Proposed scheme is equally good for color as well as gray scaled images. Another interesting aspect of this research is that it implicitly presents fusion of cover and information to be hidden in it while taking care of passive attacks on it.**

Keywords*—*Steganography; Imperceptibility; Information Hiding; LSB Technique; Secure Communication; Information Security

I. Introduction

The word Steganography is derived from Greek means "Hidden Writing" [1] and dates back to 440 B.C. [2]. Some earlier examples as reported in [3] include: shaving scalp of a most trusted slave to etch a secret message and waiting for the hair to grow after which he was sent to allies who retrieves it by reshaving his head; engraving messages on wooden Tablet and then covering it wax. The receiver retrieves it by melting the coated wax. A comprehensive insight on unconventional steganographic schemes has well been elucidated in [4].

Steganography is an ancient art [5] that with technological revolution has now been evolved into a science [6] to avert detection of hidden data. [7] delivered terminology for steganography while Simmon [8] gave the first model for steganography by discussing the scenario of Alice and Bob held in separate prison cells had to communicate through Warden Wendy. Types of steganographic system are discussed in [9] as pure (with no Stego key), private key and public key respectively whereas three techniques for steganography including insertion, substitution and cover generation have been discussed in [10].

Cryptography, having Greek origin and with same inception period as that of steganography, means "Secret Writing" [11] the essence of which is to inarticulate secret information in contrast to steganography whose sole perseverance is to conceal the fact that such information does really exist. Though opposite to each other in their approach, these two serves well as a double edged weapon to safeguard information security frontiers [12-14].

The mammoth growth of internet as communication medium has insentiently provided an opening for surreptitious communication that has been exploited in full by academics and mavens through variety of file formats (as hidden information carrier) that exist for text, image, audio and video etc. storage and representation. This paper besides presenting an innovative secure scheme for LSB based image steganography, also expounds on predominant misconception regarding detection and that for favoring bulk of online data exchange. The paper is planned as follows:

Section II introduces reader with basics of image steganography. Following this, in Section III, is the literature review of some the most recently published research articles on LSB based steganographic schemes. Theoretical foundation to disregard misapprehension of detection of steganography is the prima facie of Section IV. Section V elaborates on the proposed secure data hiding scheme while Section VI presents test results. Misapprehension about cover's capacity is discussed in Section VII. Technical analysis of the proposed logic is given in Section VIII. Advantages of the proposed scheme are highlighted in Section IX. Future work comes in Section X and Section XI concludes the discussion.

II. Brass Tacks

An image can be thought as a logical arrangement of color(s) perceived by human as an object. A digital image on the other hand is viewed as a two dimensional function ***i***(x, y), where x and y are plane coordinators pointing to a unique value, corresponding to light's intensity [15] at that point, and stored as raw data inside persistent storage which gets its meaning from the header that precede and relates it to a specific file format e.g., BMP, JPEG, TIF etc.

Image can be stored as black and white, 8-bit (mishmash of black and white colors) as shown in Fig. 1 in the form of 8 x 32 matrix, 16-bit or 24-bit files. A 24-bit color image is expressed in terms of multiple groups of 3-bytes each analogous to red, green and blue colors called RGB colors that tally to 2 ^ 24 – 1 colors in total, but 8-bit images for steganographic purposes are more suitable because it offers steady transformation of shades (from 0 ~ 255). 16-bit images have varied RGB representations such as 5 (R), 6 (G), 5 (B) / 5, 5, 5 (excluding LSB) bits etc. [16-17].

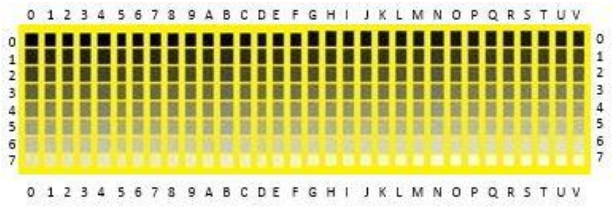


Fig. 1. 256 Shades of a Gray Scaled Image

Lossy and lossless data compression techniques are / can also be applied on images e.g. JPG etc. [18]. The former, however, may result in loss of valuable hidden information.

A. Classifying Image Steganography

Image Steganography is characterized in [19] as Spatial Domain (Plane co-ordinate system), and Transform (Frequency) Domain where former permits direct bit manipulation while for later a digital image is first transformed and then manipulated [20].

a) Spatial Domain data hiding algorithms are discussed in [21] that includes:

1) Non-filtering Algorithms – LSB replacement. Pixel Value Difference (PVD) is also being discussed for spatial domain steganography such as in [22].

2) Randomized Algorithms – Over comes drawback of sequential placement of LSB bits.

3) Filtering Algorithms – Separates Most Significant Bits (MSB) from LSB for using less significant bits for information hiding.

b) Transform Domain data hiding schemes are:

1) Discrete Cosine Transformation is the focus of research in [23-24].

2) Discrete Wavelet Transformation, for which [25] be seen

Because conversion from one domain to another is without any loss of information, hence some techniques such as follows, works well in both domains.

1) Patch Work discussed in [26-27].

2) Spread Spectrum shown in [28].

B. Attacks on Steganographic Systems

Cachin in [29] expanded on two types of errors that Wendy may commit towards detecting hidden information exchanged by Alice and Bob as follows:

a) *Type – I (False Positive) Error: Wendy detects a hidden message inside the cover where no message is sent.*

b) *Type – II (False Negative) Error: Wendy clears and let go a cover that does carry a hidden message.*

Based on above analogy any steganographic system is ought to be evolved to maximize the probability of occurrence of Type – II error.

Active and passive types of attacks are discussed in [30] where former intentionally attempts to remove hidden information whereas the later tries to extract the hidden information for analysis/retrieving hidden information from the Stego object.

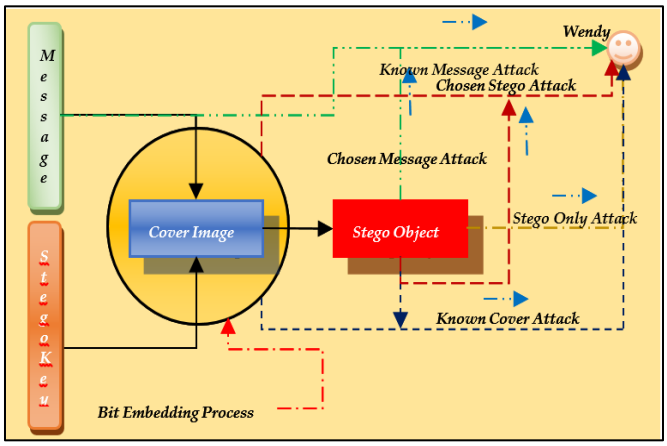


Fig. 2. Five Types of Attack on Steganographic System

[31] has categorized attacks on any steganographic system into five types depicted in Fig. 2 with a concise explanation of each as follows:

1) Chosen Message attack. Here the attacker aims to unfold the effect of embedding algorithm by choosing messages of his/her choice.

2) Chosen Stego attack. With selected Stego objects, the attacker tries to arrive at the embedding algorithm.

3) Known Cover attack. With known cover and its corresponding Stego object, an attacker attempts to contrast differences in the two to conclude on hidden information.

4) Known Message attack. Here an attacker tries to unfold the information embedding methodology by analyzing the Stego object.

5) Stego Only attack. The attacker is in possession of Stego object and tries to extract hidden information out of it.

In order for secure steganography to prevail, it is desirous that any steganographic scheme must take into account all types of attacks.

III. Literature Review

A. LSB Steganography for Digital Images

As evident from Fig. 3 that shows 8-bit gray scale image when split into corresponding eight bit planes (from low order bits to high, in sequence) - lower order bits carry subtle (visual) details about an image in contrast to high order bits. Hence, changes made in the least order bits can seldom have an impact on image appearance in general but only when analyzed in milieu of limitation of Human Visual System (HVS) [32].

Least Significant Bit Steganographic technique (for digital images) substitutes secret bit of information at least significant position of every pixel of an image i.e., 7th from left to right with most significant bit at 1st position. [33-39] presented the rudimentary manner in which LSB technique works (for further study on its progression [40-41] serves as reference) which, since then, has been experimented on varied levels of LSB positions [42-43].

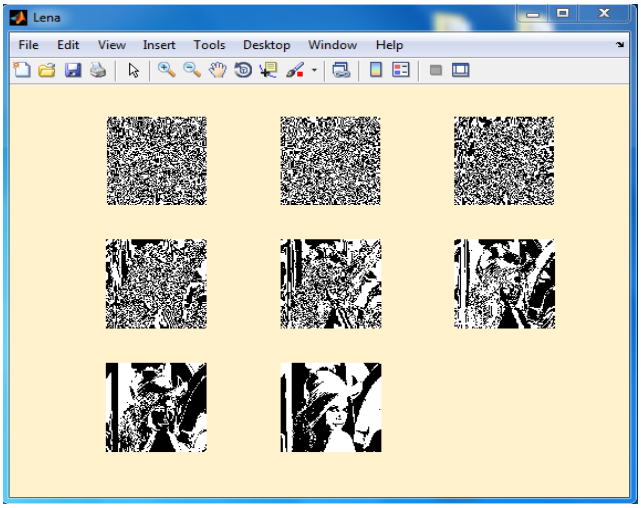


Fig. 3. Eight-bit plane slice view of an Image

Basic LSB substitution technique works as follows:

Let the following represent various shades of gray level:

"11110010 01011010 10010001 10110100 01010101 01010110 01100111 01001101" of cover image, and let letter "F" having binary "01000110"be the secret message for hiding purpose. Substituting/replacing the LSBs of the cover gives following new gray level pixel bits: "1111001<u>0</u> 0101101<u>1</u> 1001000<u>0</u> 1011010<u>0</u> 0101010<u>0</u> 0101011<u>1</u> 0110011<u>1</u> 0100110<u>0</u>". In terms of intensity, the cover image and the resultant Stego (image) object has following values:

Cover Image: 242, 90, 145, 180, 85, 86, 103, and 77

Stego Object: 242, 91, 144, 180, 84, 87, 103, and 76

, with a negligible difference of 0, 1, 1, 0, 1, 1, 0 and 1 respectively, and is imperceptible to human eye.

An aberration associated with application of LSB technique for every byte of 24-bit color (R, G, and B colors), however, is elucidated as follows:

Let "11110010 01011010 10010001" represent the 24-bit RGB representation of a particular pixel of cover image. If "010" is the secret message then after its substitution at LSB positions in RGB composition, the Stego object has the bit combination "1111001<u>0</u> 0101101<u>1</u> 1001000<u>0</u>". In terms of intensity, the cover image and the resultant Stego (image) object has following values, with a noticeable difference of 255.

Cover Image: 15882897

Stego Object: 15883152

[43] epitomized LSB substitution using secret key for bit embedding and extraction. It is, however, opined that the illustration does not have taken into account the *known cover attack* without which the appraised scheme isn't may not be regarded as secure.

[44] improvised Matching LSB scheme that according to its author has lowered probable number of alterations per pixel to 0.375 rather than 0.5. [45] offered a more generalized way of LSB matching that further reduced the aforesaid probability of altered pixels.

Pixel value difference scheme was proposed by [46] that exploits the difference of two adjacent pixels for data hiding purpose.

A noticeable outcome of research on LSB steganography [47-49] showed that histogram for simple LSB substitution appears as "pair-wise" that can be easily identified by Chi-square test.

Adaptive LSB scheme based on piecewise mapping function relating to HVS masking physiognomies is proposed by [50] while research work conducted by [51] is based the on contrast and luminance properties of HVS.

Existing LSB based/amalgamated schemes are continuously being evolved such as [52-57] etc.

B. Steganalysis

Analogous to cryptanalysis, steganalysis is the art and science of *detecting* hidden information inside a cover without the knowledge of the embedding algorithm and the key [58]. However, it is to be noted that here the word 'detection' be taken purely in context of distinguishing *actual hidden contents from any induced artifact* because of the chance of 'error' associated with steganalysis methods as shown in [59] for images that are devoid of entrenching.

Over the years a number of steganalysis methods such as [60], [61], [62], [63], [64], [65] and [66] have been proposed to counter digital steganographic schemes. Pair of Values (PoVs) are statistically analyzed by [67] that works well for contents when hidden sequentially. [68] recommended dynamic compression after LSB steganography that minimized payload detection inside cover image. [69] called for matrix embedding for increased security of steganographic schemes. [70] suggested 'flipping' of cover image in a manner that randomly transforms 50% LSB's of all pixels resulting in false estimation of cover either with or without hidden data that remained unchanged after bit embedding. Although proposed analogy as stated by its authors, is successful against accurate steganalysis methods such as RS [71], Sample Pair Analysis (SPA) [52], and Least Square Analysis (LSA) [59], the limitation of the said scheme is that estimation error tends to zero for 100% payload. It is, however, orated in context of Section 2.2 that other associated limitations of the said scheme include:

- Cover image used once must never be reused
- What is referred as random flipping (transformation) of LSBs' by the authors, in fact, seems as a linear one, and
- Scheme's non adherence to Kerckhoff's principle

IV. Theoretical Facet

A. Statement of Purpose

Before discussing security, an important aspect is to apprehend the difference between secrecy and security. Secrecy is concerned with confidentiality within certain bounds while the latter is the extent up to which attacks may be

withstand against any system. For discussion on the limitations of perfect security for steganographic systems [72] is referred.

According to [2], "in a 'perfect' system, a normal cover should not be distinguishable from a Stego object, neither by a human nor by a computer looking for statistical patterns." Going strictly with it, however, reveals that no matter how sophisticated and complex the information hiding scheme may be, none of the techniques may withstand foresaid scenario and known cover attack where the hidden information can easily be *detected* and extracted by contrasting it with the Stego object i.e., the security of the system lies in keeping 'original cover' *secret*.

So what to strive for to have a secure steganographic system? Interestingly, the foresaid limitation of prevalent steganographic techniques/schemes also explicate on *evolution of data hiding scheme that does not necessitate the need to keep original cover secret* such that comparison of cover and Stego object does not hint at actual hidden contents while still being in compliance with Kerckhoff's principle. This also serves as the *statement of purpose* for the proposed research.

B. Modus Operandi

Following expounds on the core concepts, and preliminaries for the proposed model for data hiding:

1) Exploring candidate pixel values for data hiding in an 8-bit image: In order for the proposed bit embedding methodology to work effectively the researchers experimented with 100 8-bit gray scaled images of varying shades acquired from [73] by altering their 1 or 2 LSBs. Research findings indicated that LSB substitution worked well for the luminance in the range 0 through 63, range 64 to 95 may be engaged to accommodate more message bits if deemed necessary i.e., exceptional situations. Range 96 to 255, however, leads to statistical and visual discernibility of hidden data. Fig. 4 illustrates the research findings.

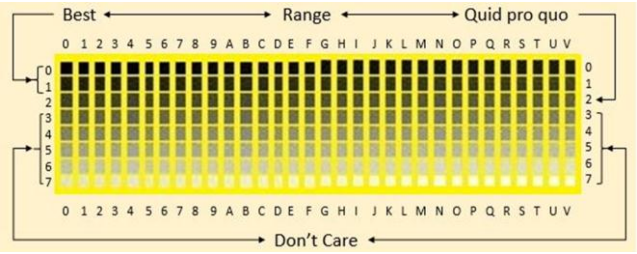


Fig. 4. Illustrating Acceptable Range of Pixel Values for LSB Secure Steganography

2) Avoiding Saturation and Wrap Around Situation

Image addition either with another image of similar dimension or a fixed value is more like an intermediary step rather than a complete process in eternity. Data retention capacity of 2-bits ranges from 0 to 3 corresponding to bit patterns {"00", "01", "10", "11"}. Since the intensity of an 8–bit grayscale image varies from 0 to 255, adding a constant value of 3 to each pixel may then results in a situation where the pixel intensity exceeds 255. Two possible scenarios for handling the overflow referred as *saturation* and *wrap around* exist respectively with their situational based (in context of choice of image) limitations which are graphically illustrated in Fig. 5.

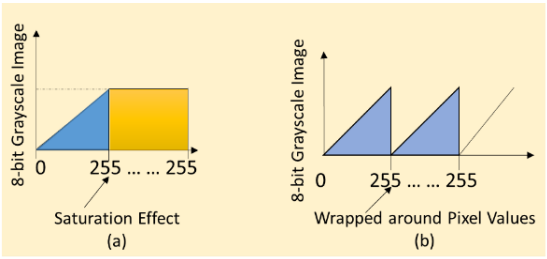


Fig. 5. Saturation and Wrapping around situations

Reducing higher values ≥ 256 to 255 as shown in Fig. 5(a) is constraint with increased illumination whereas wrapping around those values (i.e., $P_{x,y}$ MOD *256, x =0,1,2,…, N; y =0,1,2,…, M*) as illustrated in Fig. 5 (b) tends towards image darkening. To avoid saturation and wrap around situation the researchers assent on drifting the offset of an image but only for pixels having intensity ≤ 63 leaving rest of the pixels unchanged. This is so because binary equivalent of 63 is "0 0 1 1 1 1 1 1" and changing one/two LSBs shall always result in a pixel value ≤ 63.

In secret message bit embedding either for single or 2-bit pair (*obtained vide Stego key dependent processing explained subsequently*), the same shall be substituted in target pixel at LSB position(s) accordingly.

3) Message Header:

To ensure secrecy and reliability of hidden information referred to as 'C' (confidentiality) and 'I' (integrity) traits of information security, it was preferred to use Stego key dependent random substitution of one or two LSBs of cover image with encrypted header and message bits {using XoR Encryption i.e., (Header + message) XoR Stego Key} where the header comprises of secret message's length, its computed HASH (using SHA-256 [74] - digitally signed using RSA [75]), and file type i.e., file's extension. For XoR encryption, if the collective message bits exceed Stego key bits, HASH of the later gets recomputed (by treating previously calculated HASH as new Stego Key) and the continuing with the process. Table 1 reflects on the composition of message header.

TABLE I. MESSAGE HEADER WITH HIDDEN ENCRYPTED DATA

--- 32 bits ---	--- 32 bits ---	---- 32 bits ----	---(8 x N) bits---
Length of Secret File	Secret File's Extension	*Digital Signature* **HASH**	**Data**

4) Stego Key: 256-bit (32 Bytes) Stego Key (must be random).

5) Pseudo Random Number Generator: Details are beyond the scope of this submission.

6) Model:

To achieve the set goal of secure steganography, model proposed by [76] which is a consequent of the research presented in [77] and [78] respectively is preferred. The researchers, however, have opted for parallel processing to

induce randomness for pixels (in range 0 to 63) that remained unaltered during bit embedding process as shown in Fig. 6.

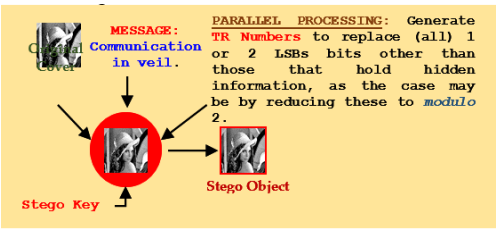


Fig. 6. New Steganographic Model for LSB Image Steganography

7) Parallel Processing of Cover:

In order to poise the effect of substitution latent uncertainty was induced by generating one/two random bits using Stego key dependent Pseudo Random Number Generator (PSNR) that gets substituted as LSBs for those pixel that fall under OFF/'0' Stego key bits (as explained in lateral discussion) during bit embedding process.

8) Pseudo Random Number Generator (PRNG):

Fig. 7 explicate on the PSNR used during bit embedding and extraction process further details of which are beyond the scope of this paper.

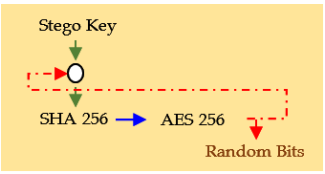


Fig. 7. Pseudo Random Bit Generation Process

V. Proposed Algorithm

A. Information Embedding Process

a) Select cover Image.

b) Select secret file that is to be hidden inside selected cover.

c) Determine HASH of secret file and encrypt the same using sender's private key.

d) Join secret message length, file's extension along with its digital signature (encrypted HASH) and affix it as message header at the beginning of the secret message.

e) Exclusive-Or the outcome of step (d) with Stego key.

f) Outcome of preceding step serves as "ready-to-get-embedded inside cover" information.

g) Compute and store as follows:

$$b1(i-1)=(Stego.Key(i-1)+Stego.Key(i)) \ MOD\ 2+1,\ i=1 \ldots 31 \quad \ldots (1)$$

$$b1(31)=(Stego.Key(0)+Stego.Key(31)) \ Mod\ 2+1 \quad \ldots (2)$$

i.e., b1(0..31) = 1 or 2, indicates how many LSBs of selected target locations in original cover are to be replaced with secret message bits.

Note: For 1-bit implementation, MOD 2 + 1 be replaced with MOD 2, where no LSB substitution for b1(i)=0.

h) Select a 256-bit random secret Stego key and translate it into its equivalent binary. Concatenate 256 Stego key bit blocks one after another till that length becomes equal to or greater than the length of the cover file.

i) Calculate Stego key dependent random pixel within the selected cover using equations (3) and (4).

$$d = (d + \sum_{i=0}^{31} \left(Stego.key_i^3 \right) \bmod 65535) \bmod 65535 + 1 \quad \ldots \ldots \ldots (3)$$

$$d = Length.of.Cover / d + 1 \quad \ldots \ldots \ldots (4)$$

j) Starting from the random pixel 'd' traverse the cover file sequentially but in cyclic order just before the pixel 'd' while performing the following steps:

- Find pixel value in range 3 to 66.
- Take the binary bits of Stego key blocks one-by-one and for ON/'1' bit, check in sequence, the number of bits corresponding to b (i) where i = 0 to 31. Take the same number of secret message bits and substitute those at LSB position(s) of targeted pixel. The index 'i' gets reinitialized to zero if secret bits are still left for embedding. Terminate bit embedding process once all secret bits get exhausted.
- Repeat the process till the secret file get hidden inside the cover image file.

B. Bit Extraction Process

a) Select Stego object.

b) Select pre agreed secret 256 bit Stego key and convert it into its equivalent binary.

c) Compute and store as given in Sec. V (A)(g).

d) Calculate Stego key dependent random pixel within the selected cover as given in para (i) of Sec. V (A).

e) Taking the value of 'd' form preceding step perform the following till extraction of 96 bits i.e., hidden message header:

- Find pixel value in range 0 to 63.
- Take the binary bits of Stego key blocks one-by-one and for its ON/'1' bit check in sequence the number of bits corresponding to b (i) where i = 0 to 31. Extract (and thereafter concatenate) the same number of bits from target pixel of Stego object.
- Aforesaid process be repeated up to length of message (8 x message length) arrived at via message header explained subsequently.
- Outcome i.e., 96 bits from preceding step gets exclusive-Or (XoR) with Stego key which gives concealed header.
- Extract hidden message's HASH using sender's public key and the outcome be stored for subsequent usage.

- Compute HASH of the extracted hidden information.
- If the computed HASH equates to one obtained from then non-repudiation of the sender also gets established besides confirming the integrity of hidden information.
- Store the extracted bits in a file (which was hidden in the cover image). Assign it a name and post fix the extracted extension (from the header) to it.

C. Illustration

Following is a step by step illustration of secret message bits embedding and extraction process using "Parrot.Jpg"- well-known in image processing, which along with its histogram appears in Fig. 8.

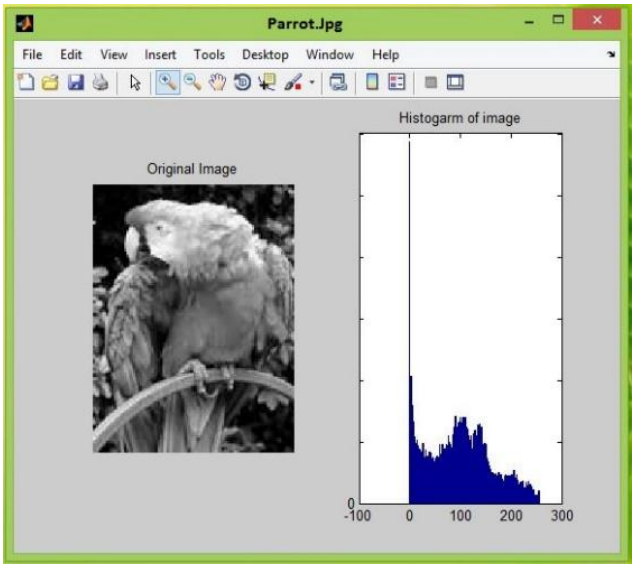


Fig. 8. Image Parrot.jpg along with its Histogram

1) Bit Hiding Process

- Let Fig. 9 represent a portion of the cover image for exemplification purpose where encircled in red are the possible target pixel values for holding secret message bits.
- Let the secret message be "Al-Awra" comprising of 7 characters which in terms of number of bits equate to 56 (7 x 8). The message is of type "Text", its binary equivalent is: "01000001- 01101100- 00101101- 01000001- 01110111- 01110010- 01100001" for corresponding ASCII values "65, 108, 45, 65, 119, 114, and 97" respectively. Computed HASH (SHA 256) of the message in hexadecimal Format (to be encrypted using Sender's Private key) is as under:

  "c58c23e9aad108e423e2ad0ccb261c7563e03f
  b9a6a31217aa25c2cb905640d7"
- The first four bytes of computed HASH shall be a part of message header.
- Let the secret 256-bit Stego key in hexadecimal format be as follows:

  3F613BCD5AF1FCA223EC42477DA7CD7CAE425
  439B3CA1A15405980D0C0BAE464

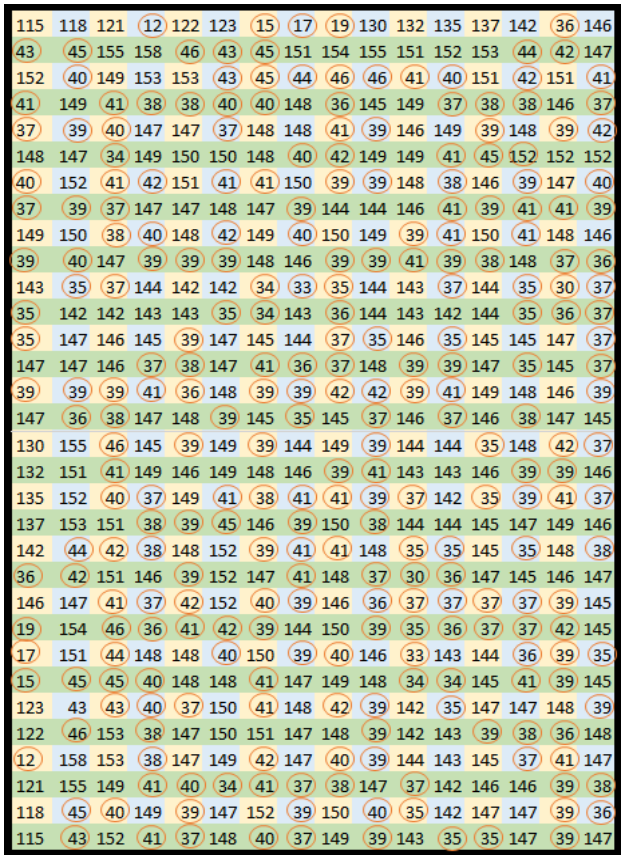


Fig. 9. Randomly Extracted Darkish Portion of the Cover Image

- Binary equivalent of which is as follows:

  00111111 01100001 00111011 11001101 01011010 11110001 11111100 10100010 00100011 11101100 01000010 01000111 01111101 10100111 11001101 01111100 10101110 01000010 01010100 00111001 10110011 11001010 00011010 00010101 01000000 01011001 10000000 11010000 11000000 10111010 11100100 01100100

I) Equations (1) and (2) render the following numbers for bit substitution by operating on the Stego key, which is an input to bit embedding process:

1 1 1 2 2 2 1 2 2 1 2 1 1 1 2 1 1 1
2 1 2 1 2 2 2 2 1 1 1 1 1 2

i.e., 32 target pixels shall hide 46 encrypted bits.

II) From equations (3) and (4), 'd' is computed as 33130 for 512 pixel values, and is indicated in blue in Fig. 10.

- *From preceding steps, the message header takes the form as follows ("-" is only used for clarity):*

7 46-84-88-84 197-140-35-233

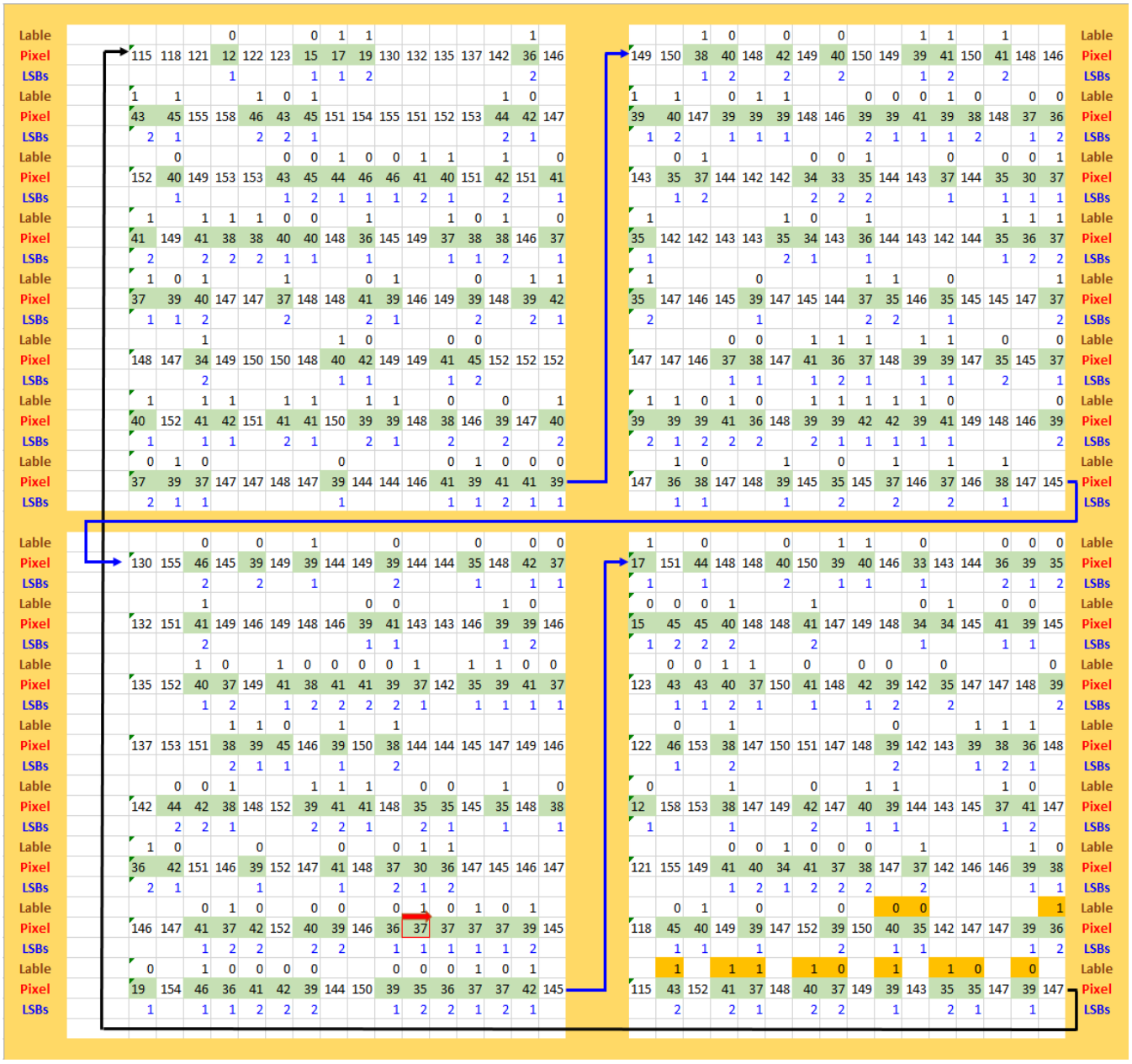


Fig. 10. Illustrating Target Locations along with Number of Secret Bits for Embedding

Fig. 10 depicts the target pixels labeled as '1' where number of bits to be hidden is written immediately below-the respective target pixel value. Pixels labelled as '0' are *don't embed* locations whose one/two LSBs will be randomly populated using PRNG in parallel with actual encrypted bit embedding processing.

- Affixing header with the secret message takes the following form when represented in binary form and totals 152 bits:

- 00000000000000000000000000000111001010111001010100010110000101010011000101100011000010001111101001010000010110110000010110101000001011101110111001001100001

This gets '*Exclusive Or*' (XoR) with the stego key bits as follows:

00111111011000010011101111001101010110
⊗ 00000000000000000000000000000111001011
00111111011000010011101111001010011101

10111100011111111001010001000100011110
⊗ 10010101000101100001010100110001011000
00101001011010010011110110111001100110

11000100001001000111011111011010011111
⊗ 11000010001111101001010000010110110000
00000110000110101110001111001100101111

00110101111100101011100100001001010100
⊗ 10110101000001011101110111001001100001
10000000111101110110010011000000110101

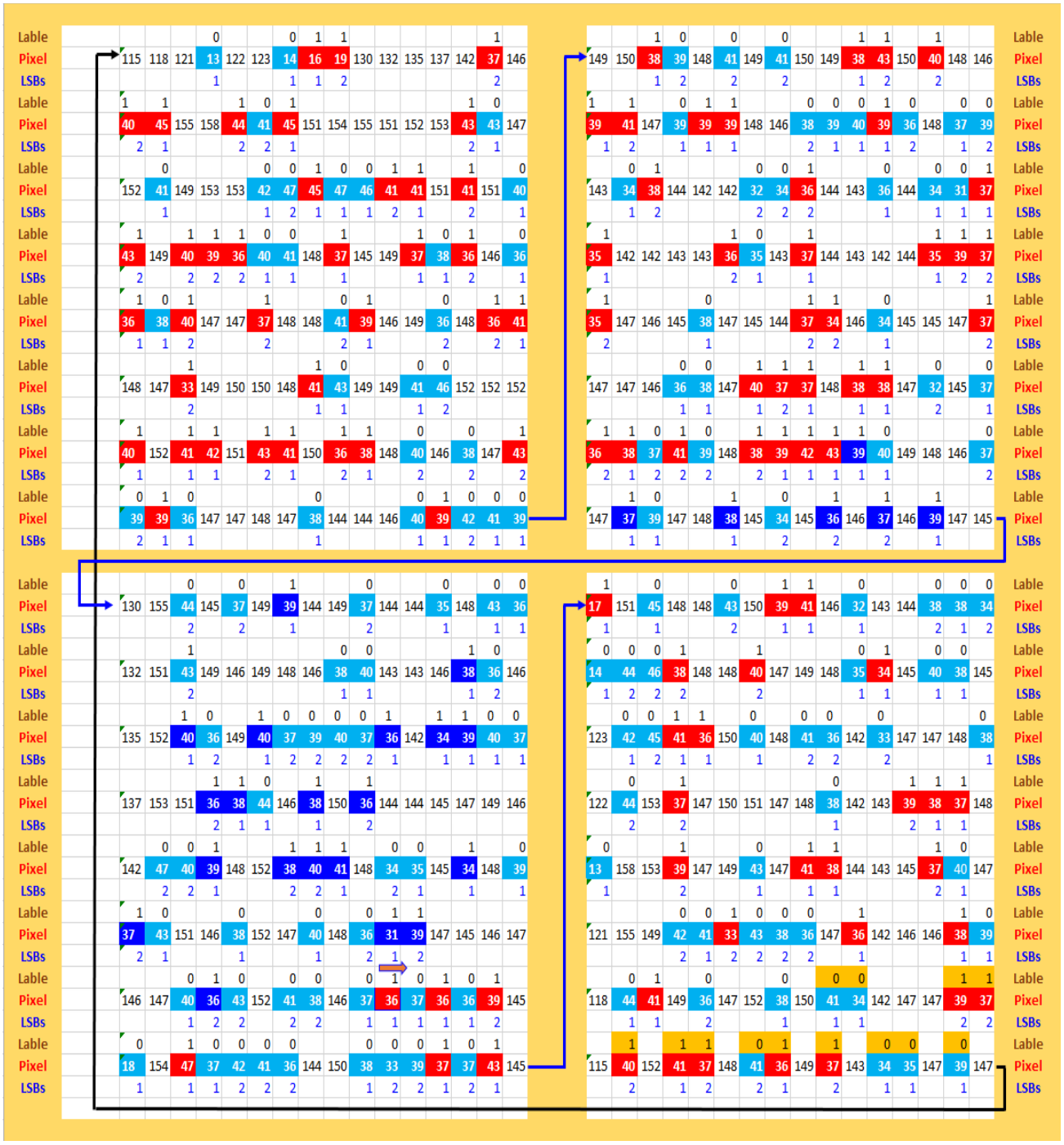
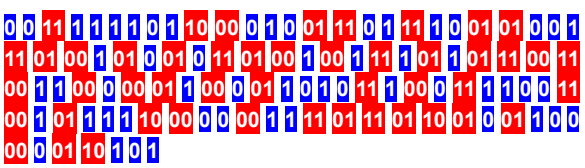


Fig. 11. Illustrating Outcome of Bit Embedding Process

and the outcome (given below) serves as ready-to-embed encrypted secret bits:

```
00111111011000010011101111001010011101
00101001011010010011110110111001100110
00000110000110101110001111001100101111
10000000111101110110010011000000110101
```

- Following is the Stego key dependent splitting of encrypted message bits (with Header inclusive) for substituting the LSBs of target pixels in the cover on the analogy portrayed vide Fig. 9.



115	118	121	13	122	123	14	16	19	130	132	135	137	142	37	146
40	45	155	158	44	41	45	151	154	155	151	152	153	43	43	147
152	41	149	153	153	42	47	45	47	46	41	41	151	41	151	40
43	149	40	39	36	40	41	148	37	145	149	37	38	36	146	36
36	38	40	147	147	37	148	148	41	39	146	149	36	148	36	41
148	147	33	149	150	150	148	41	43	149	149	41	46	152	152	152
40	152	41	42	151	43	41	150	36	38	148	40	146	38	147	43
39	39	36	147	147	148	147	38	144	144	146	40	39	42	41	39
149	150	38	39	148	41	149	41	150	149	38	43	150	40	148	146
39	41	147	39	39	39	148	146	38	39	40	39	36	148	37	39
143	34	38	144	142	142	32	34	36	144	143	36	144	34	31	37
35	142	142	143	143	36	35	143	37	144	143	142	144	35	39	37
35	147	146	145	38	147	145	144	37	34	146	34	145	145	147	37
147	147	146	36	38	147	40	37	37	148	38	38	147	32	145	37
36	38	37	41	39	148	38	39	42	43	39	40	149	148	146	37
147	37	39	147	148	38	145	34	145	36	146	37	146	39	147	145
130	155	44	145	37	149	39	144	149	37	144	144	35	148	43	36
132	151	43	149	146	149	148	146	38	40	143	143	146	38	36	146
135	152	40	36	149	40	37	39	40	37	36	142	34	39	40	37
137	153	151	36	38	44	146	38	150	36	144	144	145	147	149	146
142	47	40	39	148	152	38	40	41	148	34	35	145	34	148	39
37	43	151	146	38	152	147	40	148	36	31	39	147	145	146	147
146	147	40	36	43	152	41	38	146	37	36	37	36	36	39	145
18	154	47	37	42	41	36	144	150	38	33	39	37	37	43	145
17	151	45	148	148	43	150	39	41	146	32	143	144	38	38	34
14	44	46	38	148	148	40	147	149	148	35	34	145	40	38	145
123	42	45	41	36	150	40	148	41	36	142	33	147	147	148	38
122	44	153	37	147	150	151	147	148	38	142	143	39	38	37	148
13	158	153	39	147	149	43	147	41	38	144	143	145	37	40	147
121	155	149	42	41	33	43	38	36	147	36	142	146	146	38	39
118	44	41	149	36	147	152	38	150	41	34	142	147	147	39	37
115	40	152	41	37	148	41	36	149	37	143	34	35	147	39	147

Fig. 12. Stego Object (Image's Pixel Values) Carrying Hidden Information

- Fig. 11 shows the outcome of bit embedding where pixels values enclosed in red square contains hidden message bits. Pixels that are under label '1' but does not carry hidden data together with those that fall under label '0' are enclosed in color other than white. These are the pixels values whose 1 or 2 LSBs are substituted with randomly generated 1 or 2 binary bits using Stego key dependent PRNG.

2) Bit Extraction Process

- Let the received Stego object byte values be as shown in Fig. 12.
- The pre agreed secret Stego key is `3F613BCD5AF1FCA223EC42477DA7CD7CAE425439B3CA1A15405980D0C0BAE464`, its corresponding binary equivalent bits and 1 or 2 bit patterns obtained via equations (3) and (4) are:

1) Binary equivalent Bits:

```
00111111 01100001 00111011 11001101
01011010 11110001 11111100 10100010
00100011 11101100 01000010 01000111
01111101 10100111 11001101 01111100
10101110 01000010 01010100 00111001
10110011 11001010 00011010 00010101
01000000 01011001 10000000 11010000
11000000 10111010 11100100 01100100
```

2) 1 or 2 Bit Patterns for Hidden Bits Extraction:

```
1 1 1 2 2 2 1 2 2 1 2 1
1 1 2 1 1 1 2 1 2 1 2 2
2 2 1 1 1 1 1 2
```

- The random Stego key dependent starting point with in stego object for bit extraction obtained via equations (5) and (6) respectively is $d = \mathbf{33130} \bmod 512 + 1 = 363$, where 512 is the length of Stego object (File).

- In order to extract only the required hidden information and to avoid unnecessary processing of irrelevant data it is ought to first extract 96 bits of hidden message Header that gives hidden information's length, its type, and expected HASH. Hence, commencing from pixel $d = 363$ and proceeding forward in cyclic order the first 96 hidden LSBs of targeted pixels gets extracted using procedure explained bit hiding process and as illustrated in Fig. 13.

1) Hidden Extracted LSBs f targeted pixels:

2) Extracted hidden bits are then XoR with first 96 bits of Stego key that yields message's:

Length (i.e., 7)

```
  0011111101100001 0011101111001101
⊗ 0011111101100001 0011101111001010
  0000000000000000 0000000000000111
```

Type (i.e., .TXT)

```
  0101101011110001 1111110010100010
⊗ 0111010010100101 1010010011110110
  0010111001010100 0101100001010100
```

HASH (i.e., First four Hex bytes: c58c23e9)

```
  0010001111101100 0100001001000111
⊗ 1110011001100000 0110000110101110
  1100010110001100 0010001111101001
```

3) After extracting and decrypting Header information the process continues for the next 56 bits which are then XoR with Stego key bits from 97th bit onwards as shown below.

```
  01111101 10100111 11001101
⊗ 00111100 11001011 11100000
  01000001 01101100 00101101

  01111100 10101110 01000010
```

⊗ 00111101 11011001 00110000
01000001 01110111 01110010
01010100
⊗ 00110101
01100001

i.e.

01000001 01101100 00101101
01000001 01110111 01110010
01100001

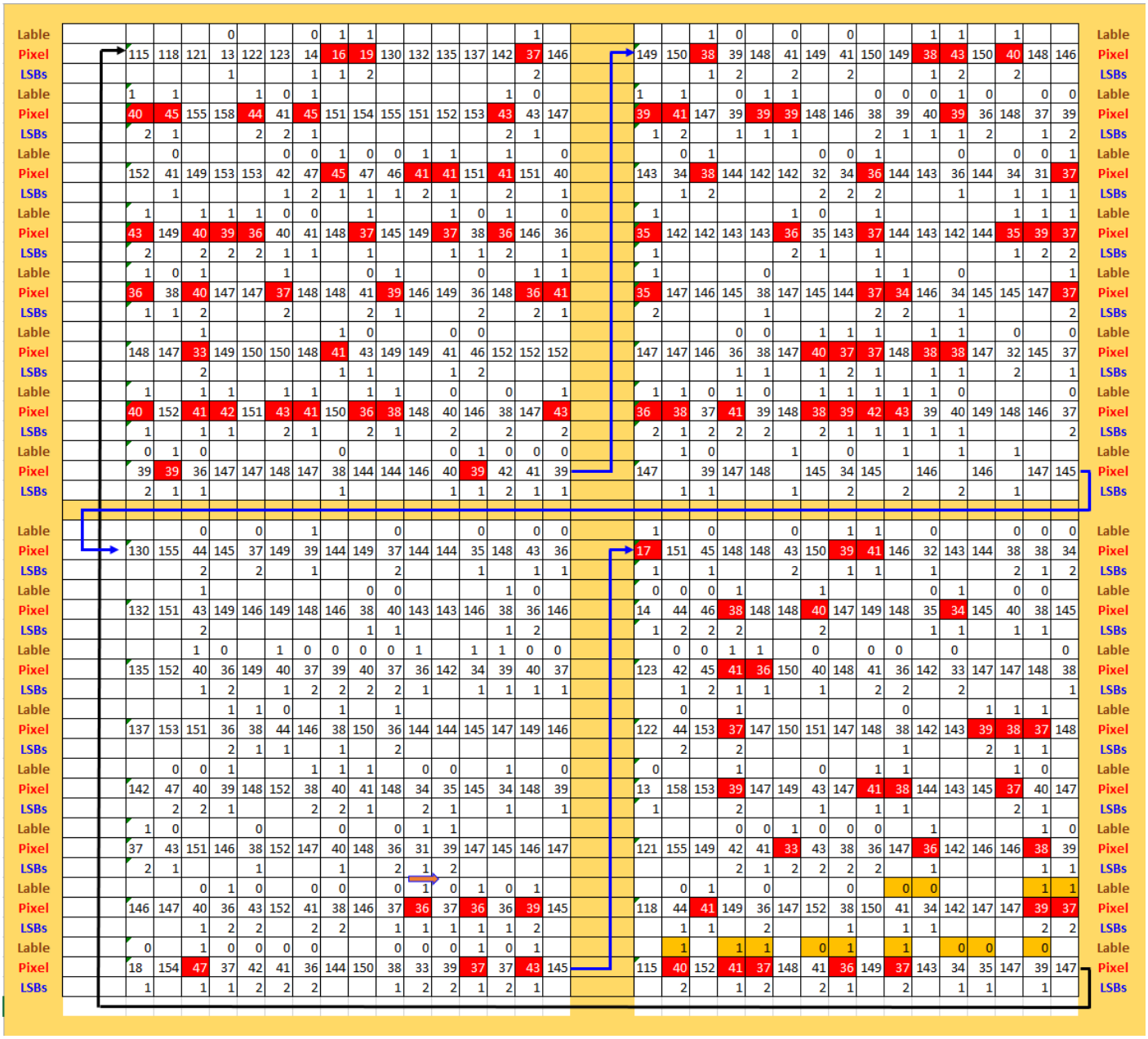


Fig. 13. Hidden Bits Extraction Process

4) The resultant bits are concatenated in chunks of length 8 each, and are then translated into equivalent ASCII character codes as "Al-Awra", that are saved in a file having extension ".TXT".

5) To confirm on the integrity and non-repudiation of message/hidden information the received contents are subjected to SHA-256 HASH algorithm (followed by its decryption using Originator's Public key) the outcome of which is

"c58c23e9aad108e423e2ad0ccb261c7563e03fb9a6a3
1217aa25c2cb905640d7"

, where the first four bytes are the same as that extracted from hidden message's header thereby affixing on the legitimacy of the message as well as of its sender.

Mean, variance and standard deviation for the aforesaid illustration were computed as given in Table 2 while its graphical representation are as shown in Fig. 14 respectively.

Mean square error and Peak signal-to-noise ratio of the cover and stego object are as shown in Table 3.

TABLE II. MEAN, VARIANCE AND STANDARD DEVIATION FOR COVER AND STEGO OBJECT

OUTCOME	Cover Pixels	Stego Object
Mean	0.8910938	0.8897656
Variance	29.2351052	29.3776853
Standard Deviation	0.540695	0.5420119

TABLE III. MSE AND PSNR FOR COVER AND STEGO OBJECTS

Image	Dim	LSBs	MSE	PSNR
Lena.jpg	512 x 512	1	0.499097936447318	51.1489458661669
		2	2.49174973991598	44.1657593926575
Monalisa.jpg		1	0.498689440540415	51.1525018848588
		2	2.53367308343121	44.0932978316228
Parrot.jpg		1	0.503298725650196	51.1125453010079
		2	2.51557345741172	44.1244335716171

VI. TEST RESULTS

Fore test purposes we selected three freely available (on web) 512 x 512 sized 8-bit gray scaled "jpg" images as shown in Fig. 15.

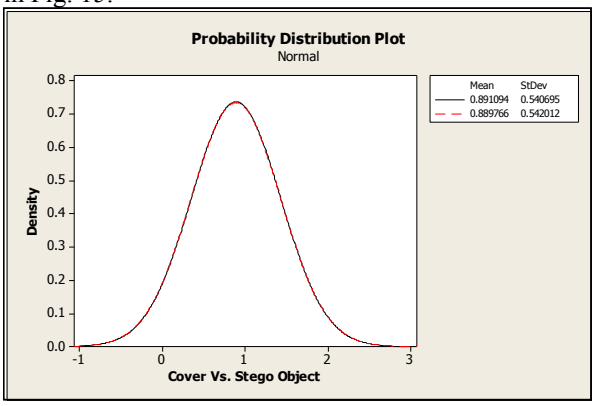


Fig. 14. Contrasting Cover and Stego Object


Lena.jpg


Monalisa.jpg


Parrot.jpg

Fig. 15. Test Images

"Communication in veil." was our secret message that equals 176 bits in total and was concatenated with 96 bits of header information. We opted to test the efficiency of our proposed solution by observing the quantified effect of 1 and 2-bit LSB change induced by bit embedding on the selected cover (image). In this connection cover image, parallel processed Cover and Stego object were subjected to two of the five full-reference algorithms that serves as fundamental components of Image Quality Assessment (IQA) [79] delineated subsequently, and the source code of which is available at [80]:

a) Mean Squared Error (MSE): Depicts the amount of biasing in an image. It is computed using formula as shown in equation (5), where the higher the value of MSE the higher will be the distortion.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(Y_i - \tilde{Y}_i\right)^2 \qquad \textbf{(5)}$$

b) Peak Signal-to-Noise Ratio (PSNR): As the name implies PSNR is the ratio between extreme power (possible value) of a signal and the power of garbling noise that affects the quality of that signal. The formula for computing PSNR is as shown in equation (6):

$$PSNR = 20\log_{10}\left(\frac{MAX}{\sqrt{MSE}}\right) \qquad \textbf{(6)}$$

- The effect is graphically elucidated by plotting the probability distribution graph of the original (image) cover and parallel processed cover/stego object (for the three images referred in Fig. 15) using Minitab 16 [81] as illustrated in Fig. 16-21, via computing their mean, variance and standard deviation shown in table 4 respectively.

TABLE IV. MSE AND PSNR FOR COVER AND STEGO OBJECTS

Lena.jpg		Mean	Variance	Standard Deviation
Original Image		1.2404707	22.6704645	0.4761351
Stego Object	1	1.2404602	22.6773109	0.476207
	2	1.2403668	22.6849972	0.4762877

Monalisa.jpg		Mean	Variance	Standard Deviation
Original Image		0.5603488	16.0417024	0.4005209
Stego Object	1	0.5604179	16.0390902	0.4004883
	2	0.5605014	16.0517136	0.4006459

Parrot.jpg		Mean	Variance	Standard Deviation
Original Image		0.9716536	40.1667786	0.6337727
Stego Object	1	0.9718385	40.1481114	0.6336254
	2	0.9718984	40.1030232	0.6332695

VII. DELUSION ASSOSIATED WITH COVER CAPACITY IN CONTEXT OF SECURE COMMUNICATION

Since inception of digital steganography, images have remained a preferred choice for cover or as hidden information carrier by virtue of having the Meta data / redundant associated information (purely in terms of bit's significance towards overall appearance). However, in context of security, a digital

object with more of hidden information may indirectly explicate on bit embedding algorithm especially when the same cover is repeatedly used as carrier in communication. [82] acmes on the implication of putting more information online that needs to be taken seriously in its eternity while evolving secure steganographic schemes or other security system.

VIII. Technical Analysis

Let $\varepsilon(\theta)$ denotes the entropy of Cover Image while $\varepsilon(\varphi)$ represents that of the Stego Object. Clearly if $\varepsilon(\theta) = \varepsilon(\varphi)$ after bit hiding then it implies that original Cover remains unaffected by the bit embedding process which, however, is a rare case to occur. Hence, for all remaining cases, $\varepsilon(\theta) \neq \varepsilon(\varphi)$ implies that the difference between Cover and Stego Object point towards hidden information i.e., $\varepsilon(\theta) - \varepsilon(\varphi)$ = Hidden Information either with or without using encryption, and as apparent is unsecure. So in order for secure steganography to prevail, we ought to devise some scheme such that $\varepsilon(\theta) - \varepsilon(\varphi)$ does not point directly towards hidden information i.e., $\varepsilon(\theta) - \varepsilon(\varphi) = \delta(\square)$, where $\square$ represents a mix of hidden information and statistically related random bits arrived at via some random source/process under control of Stego key $\delta(\square) = E_{mbed}$(StegoKey, Secret Data/Information, Random.Bits=μ(Random)), which is also analogous to Kerckhoff's Principle.

It is apparent that our proposed methodology is in confirmation with the aforesaid argument and hence poses a hard to solve problem for Wendy constraint only by the time and resources she is willing to invest.

IX. Advantages

Following are some of the advantages of proposed scheme:

a) Secure

b) Aptness for colored images.

X. Future Work

a) Bench marking of gray scaled Images that are suitable as Cover for the proposed data hiding scheme.

b) Research work on AVI Steganography based on proposed scheme is in process.

XI. Conclusion

This research endeavor is This research endeavor is amongst those of the few image based steganographic schemes that does not necessitate on having original (cover) image at receiver's end for extracting hidden information while use of TRNG distinct it from the rest of its counterparts. A salient feature of the proposed scheme is that it is equally suitable for gray scaled and as well as for colored images (when implemented for 'B' – Blue color). It can be easily inferred from the test results that secret message is diffused in the cover, by virtue of preprocessing of image and random scattering of message bits, in such a manner that attacker may not even precise as to whether or not the image carries some hidden information. All of the foresaid traits raises the probability for Wendy to commit Type II error which is desirous for any steganographic scheme.

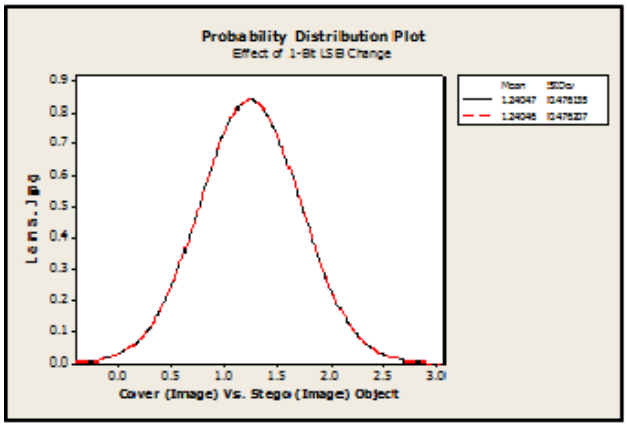


Fig. 16. Original Cover Vs, Stego Object for 1-Bit LSB Change

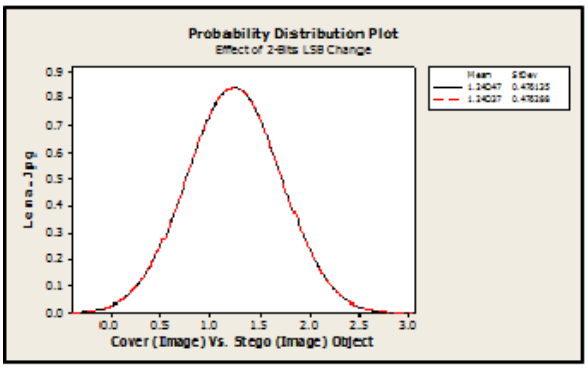


Fig. 17. Original Cover Vs, Stego Object for 2-Bits LSB Change

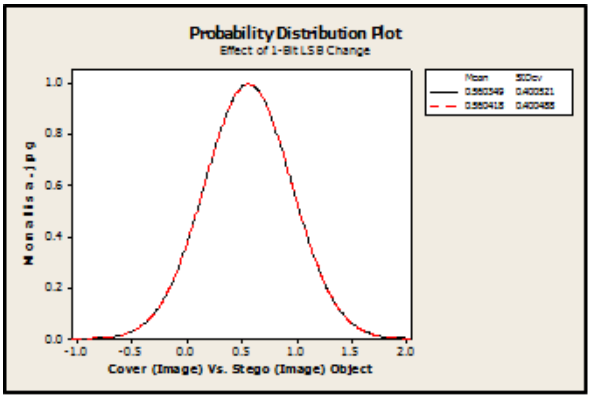


Fig. 18. Original Cover Vs, Stego Object for 1-Bit LSB Change

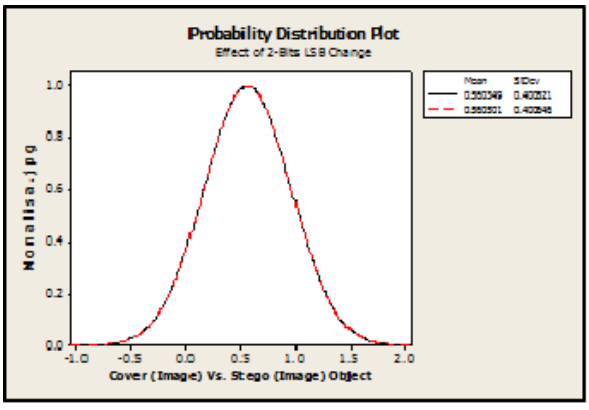


Fig. 19. Original Cover Vs, Stego Object for 2-Bits LSB Change

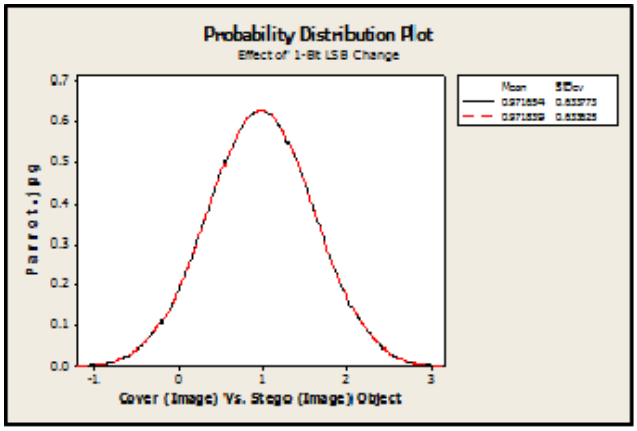


Fig. 20. Original Cover Vs, Stego Object for 1-Bit LSB Change

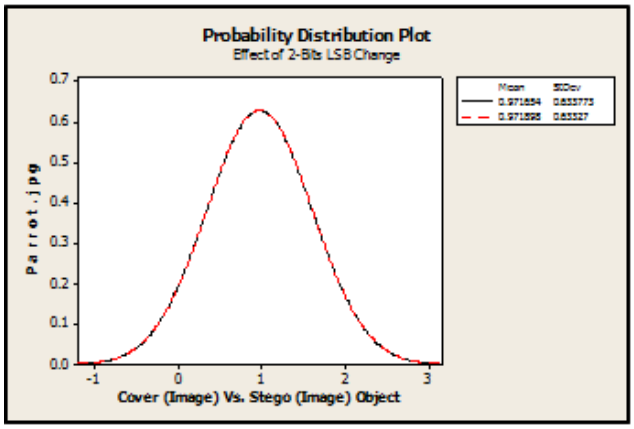


Fig. 21. Original Cover Vs, Stego Object for 2-Bits LSB Change

REFERENCES

[1] The Oxford English dictionary: being a corrected re-issue, Clarendon Press, Oxford, 1933.

[2] Stefan Katzenbeisser and Fabien A.P. Petitcolas, Introduction to information hiding. In Information Hiding: Techniques for Steganography and Digital Watermarking, Artech House. 1-14, Boston: 2000.

[3] Krista Bennett, "Linguistic Steganography: Survey, Analysis, And Robustness Concerns For Hiding Information In Text", Cerias Tech Report 2004-13, Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086

[4] Khan Farhan Rafat and Muhammad Sher, An Eccentric Scheme for Oblivious Communication. International Journal of Computer Science Issues (IJCSI). Volume 10, Issue 4, No. 2, July 2013, Pp. 89-96. www.ijcsi.org Impact Factor 0.242

[5] Neil F. Johnson, Sushil Jajodia,"Exploring Steganography: Seeing the Unseen", IEEE 0018-9162/98. 1998.

[6] Chincholkar A.A. and Urkude D.A. Design and Implementation of Image Steganography. Journal of Signal and Image Processing, Volume 3, Issue 3, pp. 111-113, 2012.

[7] B. Ptzmann, Information hiding terminology. In Anderson [5], pp. 347-350, ISBN 3-540-61996-8, results of an informal plenary meeting and additional proposals.

[8] G. J. Simmons, The prisoners' problem and the subliminal channel. In Advances in Cryptology: Proceedings of Crypto 83 (D. Chaum, ed.), Plenum Press, pp. 51–67, 1984.

[9] Mohammed Salem Atoum, Osamah Abdulgader Al- Rababah, Alaa Ismat Al-Attili, New Technique for Hiding Data in Audio File. International Journal of Computer Science and Network Security (IJCSNS), Vol.11 No.4, pp. 173-177, April 2011.

[10] Gregory Kipper. Investigator's Guide to Steganography. Auerbach Publications, pp. 240, October 2003.

[11] Jenny Shearer, Peter Gutmann, Government, Cryptography, and the Right to Privacy. Journal of Universal Computer Science (JUCS), Volume 2, No.3, pp. 113-135, March 1996.

[12] WIPO Copyright Treaty, 1996.

[13] Document prepared by the International Bureau, WIPO/INT/SIN/98/9, 1998. Presented at the WIPO Seminar for Asia and the Pacific Region on Internet and the Protection of Intellectual Property Rights, Singapore.

[14] T. Aura, "Invisible Communication," EET 1995, technical report, Helsinki Univ. of Technology, Finland, Nov. 1995; http://deadlock.hut.fi/ste/ste_html.html.

[15] Rafael C. Gonzalez and Richards E. Woods, Digital Image Processing, 3rd Edn., PEARSON Prentice Hall.

[16] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002.

[17] Raydhitya Yoseph, PSNR Comparison When Using LSB Steganography on Each RGB Color Component, IF 3058 Cryptography – Sem. II Year 2012/2013

[18] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[19] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.

[20] Lee, Y.K. & Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000.

[21] Juan José Roque and Jesús María Minguet, SLSB: Improving the Steganographic Algorithm LSB.

[22] Wu, D.C., Tsai, W.H. "A Steganographic method for images by pixel-value differencing," Pattern Recognition Letters 24 (June), 2003, pp. 1613–1626.

[23] Saad M. A. Al-Momen, Loay E. George. "Image Hiding Using Magnitude Modulation on the DCT Coefficients." Journal of Applied Computer Science & Mathematics, No. 8 (4), Suceava, pp. 9-14, 2010.

[24] Thekra Abbas, Zou Beiji, Maan Younus Abdullah. "Information Security Technique in Frequency Domain." International Journal of Digital Content Technology and its Applications (JDCTA), Volume 5, doi:10.4156/jdcta.vol5.issue12.35, pp. 279-289, December 2011.

[25] H S Manjunatha Reddy, High Capacity and Security Steganography Using Discrete Wavelet Transform, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6).

[26] Bender, W., Gruhl, D., Morimoto, N. & Lu, A. "Techniques for data hiding", IBM Systems Journal, Vol 35, pp. 313-336.1996.

[27] Neil F. Johnson and Sushil Jajodia. "Steganalysis of Images Created Using Current Steganography Software." Lecture Notes in Computer Science, Springer-Verlag, Vol. 1525, pp. 273-289, 1998.

[28] Marvel, L.M., Boncelet Jr., C.G. & Retter, C. "Spread Spectrum Steganography", IEEE Transactionson image processing, pp. 8:08, 1999.

[29] Cachin, C., An Information-Theoratic Model for Steganography, in Proceedings of the Second International Workshop on Information Hiding, vol. 1525 of Lecture Notes in Computer Science, pp. 306-31, Springer, 1998.

[30] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi. A Survey on Image Steganography and Steganalysis. Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, pp. 142-172, April 2011.

[31] A. Westfeld and A. Pfitzmann. Attacks on steganographic systems, in Proc. 3rd Int. Workshop on Information Hiding, vol. 1768, pp.61–76, 1999.

[32] Federal Aviation Administration. "Hearing and Noise in Aviation." Internet: http://www.faa.gov/pilots/safety/pilotsafetybrochures/media/hearing_brochure.pdf

[33] R. Z. Wang, C. F. Lin, and J. C. Lin, "Hiding data in images by optimal moderately significant bit replacement," IET Electronics Letters, vol. 36, no. 25, pp. 2069-2070, 2000.

[34] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," Pattern Recognition, vol. 34, pp. 671-683, 2001.

[35] C. K. Chan and L. M. Cheng, "Improved hiding data in images by optimal moderately-significant-bit replacement," IEE Electronics Letters, vol. 37, no. 16, pp. 1017-1018, 2001.

[36] C. C. Chang and H. W. Tseng, "A steganographic method for digital images using side match," Pattern Recognition Letters, vol. 25, pp.1431-1437, 2004.

[37] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol.37, pp. 469-474, 2004.

[38] C. C. Chang, J. Y. Hsiao, and C. S. Chan, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy," Pattern Recognition, vol. 36, pp.1538-1595, 2003.

[39] C. C. Chang, C. S. Chan, and Y. H. Fan, "Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels," Pattern Recognition, vol. 39, no. 6, pp. 1155-1167, 2006.

[40] C. C. Chang, M. H. Lin, and Y. C. Hu, "A fast and secure image hiding scheme based on lsb substitution," International Journal of Pattern Recognition and Artificial Intelligence, vol. 16, no. 4, pp. 399-416, 2002.

[41] C. C. Thien and J. C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function," Pattern Recognition, vol. 36, pp. 2875-2881, 2003.

[42] A. Ker, "Steganalysis of LSB Matching in Gray scale Images," IEEE Signal Processing Letter, vol. 12, no.6, pp. 441-444, June 2005.

[43] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," IEEE Transactions on Infomation Forensics Security, vol. 5, no. 2, pp.201 -214, 2010.

[44] Fridrich, J., Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press (2009).

[45] J. Mielikainen, "LSB matching revisited," IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287, 2006.

[46] X. Li, B. Yang, D. Cheng, and T. Zeng, "A generalization of LSB matching," IEEE SignalProcessing Letters, vol. 16, no. 2, pp. 69-72, 2009.

[47] D.C. Wu, W. H. Tsai (2003), "A Steganographic Method for Images by Pixel-Value Differencing", Pattern Recognition Letter, Vol. 24, No. 9-10, p. 1613–1626.

[48] Westfeld and A. P¨Tzmann (1999), "Attacks on Steganographic Systems - Breaking the Steganographic Utilities Ezstego, Jsteg,Steganos, and S-tools-and Some Lessons Learned", In Proceedings of the 3rd Information Hiding Workshop, volume 1768 of LNCS, pages 61-76. Springer, 1999.

[49] Niels Provos and Peter Honeyman (2002), "Detecting Steganographic Content on The Internet". In Proceedings of NDSS'02: Network and Distributed System Security Symposium, pp1-13, Internet Society, 2002.

[50] Stanley, C.A. (2005), "Pairs of Values and the Chi-squared Attack", in CiteSteer. 2005, pp. 1-45.

[51] Wen-Nung Lie, Li-Chun Chang (October 24-28, 1999), "Data hiding in images with adaptive numbers of least significant bits based on thehuman visual system." In Proc. IEEE Int. Conf., Image Processing. Kobe (Japan), pp 286-290.

[52] Lee, Y. K., Chen, L. H. (2000), "High Capacity Image Steganographic Model", IEEE Proc., Vis. Image Signal Process, Vol. 147, no. 3, p. 288-294.

[53] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min Sun (2008), "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems". IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, pp. 488-497.

[54] W. Luo , F. Huang and J. Huang (2010), "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp.201 -214.

[55] J. C. Joo, T. W. Oh, H. Y. Lee, H. K. Lee (Jan, 2011), "Adaptive Steganographic Method Using the Floor Function with Practical Message Formats," International. Journal of Innovative Computing, Information and Control, Vol. 7, No. 1, pp. 161-175. ISSN 1349-4198.

[56] Mandal, J.K., Khamrui, A. (2011), "A Data-Hiding Scheme for Digital Image Using Pixel Value Differencing (DHPVD)", Electronic System Design (ISED), International Symposium, pp: 347 - 351.

[57] P. Mohan Kumar, K. L. Shunmuganathan (2012), "Developing a Secure Image Steganographic System Using TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate", Information Security Journal: A Global Perspective, Vol. 21, Issue 2.

[58] Youssef Bassil (December, 2012),"Image Steganography Based on a Parameterized Canny Edge Detection Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 60– No.4.

[59] Rocha, A. and Goldenstein, S. Steganography and steganalysis in digital multimedia: Hype or hallelujah? Journal of Theoretical and Applied Computing (RITA) 15, 1, pp. 83-110, 2008.

[60] A. Ker, "Derivation of error distribution in least squares steganalysis," IEEE Transactions on Information Security and Forensics, vol. 2, pp.140–148, 2007.

[61] R. Du J. Fridrich and L. Meng, "Steganalysis of lsb encoding in color images," Proceedings of IEEE International conference on Multimedia and Expo New York City, NY, Jul 30 - Aug2, 2000.

[62] M. Goljan J. Fridrich and R. Du, "Detecting lsb steganography in color and grey-scale images," Magazine of IEEE multimedia, Special Issue on Security, October-November issue, 2001.

[63] X Wu S Dumitrescu and Z Wang, "Detection of lsb steganography via sample pair analysis," IEEE Transactions on Signal Processing, vol. 51, No.7, pp. 1995–2007, 2003.

[64] Z. Tao and P. Xijian, "Reliable detection of lsb steganography based on the difference image histogram," Proc. IEEE ICAAP, Part III, pp. 545–548, 2003.

[65] Q.Tang P.Lu, X.Luo and L.Shen, "An improved sample pairs method for detection of lsb embedding," vol. 3200, pp. 116–127, 2004.

[66] A.D. Ker, "Improved detection of lsb steganography in greyscale images," In: Proc. The 6th Information Hiding Workshop, Springer LNCS 3200, pp. 97-115, 2005.

[67] B. Liu X. Luo and F. Liu, "Improved rs method for detection of lsb steganography," In: Proc. Information Security & Hiding (ISH 2005) workshop, Springer LNCS 3481, 508-516, 2005.

[68] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems", Proc. 3rd Information Hiding Workshop, Dresden, Germany, September 28-October 1, 1999, pp. 61-75.

[69] C. Yang X. Luo, Z. Hu and S. Gao, "A secure lsb steganography system defeating sample pair analysis based on chaos system and dynamic compensation," Proceedings of International Conference, 2006.

[70] J. Fridrich and D. Soukal, "Matrix embedding for large payloads," IEEE Transactions on Information Security and Forensics, vol. 7, pp. 12–17, 2008.

[71] Shreelekshmi R, M Wilscy and M Wilscy, "Preprocessing Cover Images for More Secure LSB Steganography," International Journal of Computer Theory and Engineering, Vol. 2, No. 4, pp. 546-551, August, 2010.

[72] Jessica Fridrich, Miroslav Goljan, and Rui Du,"Reliable Detection of LSB Steganography in Color and Grayscale Images"

[73] Khan Farhan Rafat and Muhammad Sher, On the Limits of Perfect Security for Steganography System. International Journal of Computer Science Issues (IJCSI). Volume 10, Issue 4, No. 2, July 2013, Pp. 121-126. www.ijcsi.org

[74] Boundary Detection Benchmark: Image anking, http://www.eecs.berkeley.edu/Research/Projects/CS/vision/bsds/bench/html/images.html

[75] Gadgi Sumangala, V R Kulkarni, Shridevi Sali, Sulabha Apte. "Performance Analysis of Sha-2 Algorithm with and Without Using Artificial Neural Networks." World Journal of Science and Technology - 1(12), 2011, pp.12-20

[76] RSA Algorithm - Java Implementation, www.cs.duke.edu/courses/summer04/cps001/lectures/Lecture16.ppt

[77] Khan Farhan Rafat and M. Sher, Novel Perspective for XML Steganography, Accepted and under publication in International Journal of Networks and Security (IJNS), Published by Recent Research Publication.

[78] Popa, R., An Analysis of Steganographic Techniques. The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, 1998.

[79] J.Z Llner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G.Wicke, G.Wolf. Modeling the security of steganographic systems, Proc. 2nd Workshop on Information Hiding, pp. 345-355, LNCS 1525, Springer-Verlag, Portland, 1998.

[80] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, Apr. 2004.

[81] Zhou Wang, Alan C. Bovik, Hamid R. Sheikh and Eero P. Simoncelli, The SSIM Index for Image Quality Assessment, http://www.cns.nyu.edu/~lcv/ssim/#usage

[82] MiniTab 16

[83] NSA surveillance: A guide to staying secure, http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance