American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-02, Issue-09, pp-118-126
www.ajer.org

Research Paper Open Access

A Novel Approach for Image Steganography Using Dynamic Substitution and Secret Key

Saeed Ahmed Sohag, Dr. Md. Kabirul Islam, Md. Baharul Islam
[1](Department of Computer Science and Engineering, Daffodil International University, Bangladesh)
[2](Department of Multimedia Technology and Creative Arts, Daffodil International University, Bangladesh)

Abstract: - Steganography is a system that hides information in an application cover carrier like image, text, audio, and video. Considerable amount of work has been carried out by different researchers on this subject. Least Significant Bit (LSB) insertion method was more suspicious and low robustness against attacks. The objectives of this study were to analyse various existing system and implement a dynamic substitution based Image Steganography (IS) with a secret key. Our proposed method is more difficult to attack because of message bits are not inserted in to the fixed position. In our method, the message bits are embedded into deeper layer depending on the environment of the host image and a secret key resulting increased robustness. The robustness specially would be increased against those intentional attacks which try to reveal the hidden message.

Keywords: - *I-security, Steganpgraphy, secret key, secure transmission*

I. INTRODUCTION

It is the study of techniques for hiding the existence of a secondary message in the presence of a primary message. The primary message is referred to as the carrier signal or message; the secondary message is referred to as the payload signal or message. The word steganography is derived from the Greek words ‘stegos’ meaning ‘cover’ and ‘grafia’ meaning ‘writing’ [1] defining it as ‘covered writing'. IS means information hidden exclusively inside an image. The main difference between steganography and cryptography is cryptography hide the content of the message and steganography focuses on keeping the existence of a message secret [2]. If there are more similarities between the cover image and the stego-image, it will be harder for an attacker to find out that the stego-image has important secret data hidden inside it. In recent years, enormous research efforts have been invested in the development of digital IS techniques.

In this paper, we have proposed a dynamic approach of substitution in IS where message will be embedded depending on the environment of the host image and a secret key not on the fixed position and also adjust a near bit to improve the quality of the image. It becomes more important as more people join the cyberspace revolution. Privacy and anonymity is a concern for most people on the internet. IS allows for two parties to communicate secretly and covertly. It allows for copyright protection on digital files using the message as a digital watermark. One of the other main uses for image steganography is for the transportation of high-level or top-secret documents between international governments. While it has many legitimate uses, it can also be quite nefarious. It can be used by hackers to send viruses and Trojans to compromise machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely. Military communications system make increasing use of traffic security technique which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. So we prepare and implement it for efficient and secured information transformation. The objectives of the study are to analyse various existing system and implement a dynamic substitution based image steganography with a secret key. This paper has been organized as literature review, proposed work, experiment result following by discussion and conclusion.

When a stenographic system is developed, it is important to consider what the most appropriate cover Work should be, and also how the stegogramme is to reach its recipient. For example, it is possible that an image stegogramme could be sent to a recipient via email. Alternatively it might be posted on a web forum for all to see, and the recipient could log onto the forum and download the image to read the message. In terms of development, Steganography is comprised of two algorithms, one for embedding and one for extracting. The embedding process is concerned with hiding a secret message within a cover work, and is the most carefully constructed process of the two. A great deal of attention is paid to ensuring that the secret message goes unnoticed if a third party were to intercept the cover Work. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end. The entire process of steganography for images can be presented in figure 1.

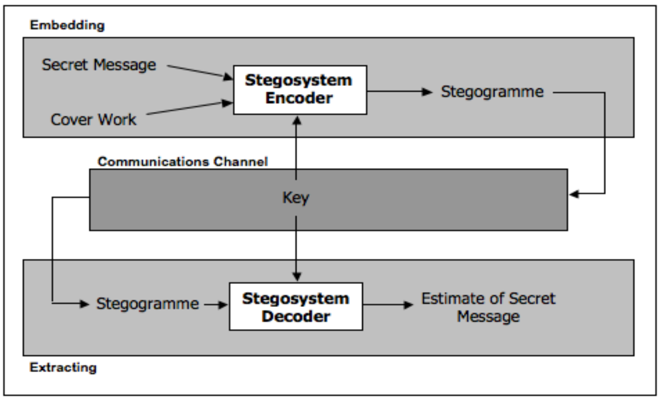


Figure 1: Block diagram of steganography process

Two inputs are required for embedding process. One is secret message that usually a text file that contains the message for transform. And cover work is used to construct a stegogramme that contains a secret message.

1.1. Stego-system

A stego-system (steganographic system) in image steganography refers to a system capable of hiding a secret message within an image, such that no third-parties are aware that the message exists. The image that is output from this process is known as a stegogramme, and great care is taken to ensure that this looks as innocent as possible so that the secret message has the best chance of reaching its intended recipient. However, the stego-system not only refers to encoding the message, it also refers to the system that makes it possible to read the message when it reaches its recipient. The two sub-systems are referred to as the stego-system encoder and the stego-system decoder respectively.

1.1.1. The Encoder

The stego-system encoder is the heart of the steganographic system. It makes it possible to embed a secret message within some cover medium. In the case of image steganography, the encoder will read in a cover image cm;n (where m and n refer to the height and width dimensions of c), and will embed a message m by tweaking carefully selected values of the cover image ci. Exactly which ci values are tweaked depends on the specific embedding algorithm, and it is this decision process that makes each stego-system unique. That is to say that replacing the image data with the message data has no direct impact on the overall perceptibility of the image, therefore meaning the message is hard to detect - at least with the naked eye. Figure 2 shows a graphical representation of the elements and processes typically associated with a stego-system encoder. Stego-systems such as these are referred to as secret key stego-systems. Of course, how many values are tweaked in c to produce the stegogramme depends on the length of the message l(m).

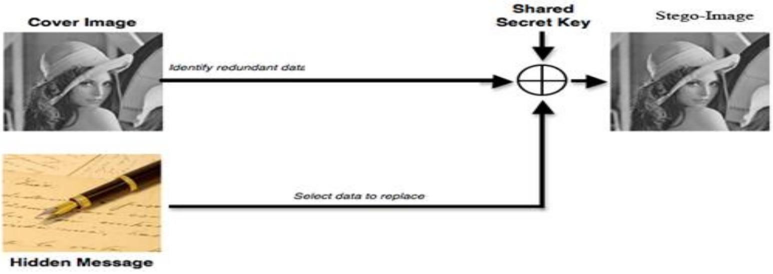


Figure 2: The general design of a basic stego-system encoder

1.1.2. The Decoder

The stego-system decoder allows the receiver of the stegogramme to obtain an estimate of the secret message m0. A good stego-system ensures that the estimate will be as close to the original message m as possible. Figure 3 shows a graphical representation of the elements and processes associated with a common stego-system decoder. As we can see, both the stegogramme and shared secret key k are used to identify the regions that hold the message data. When both of these elements are provided, each mi can be retrieved such that the complete binary sequence m0 can be constructed. The message data can then be converted to an alternative form (typically ASCII) so that it can be read.

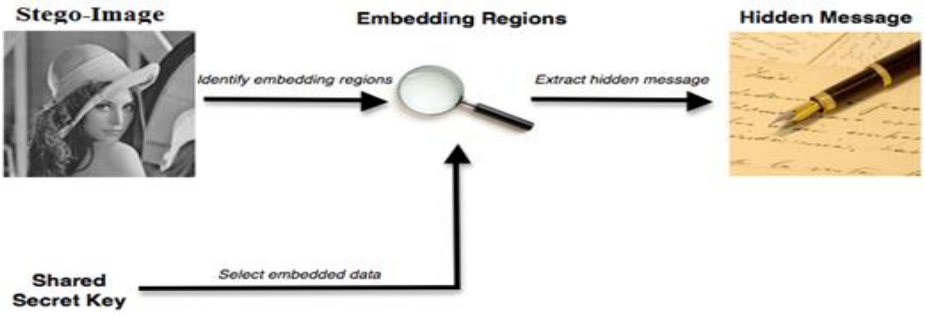


Figure 3: The general design of a basic stego-system decoder

II. RESEARCH BACKGROUND

Image steganography takes the advantage of limited power of human visual system (HVS). Here, unlike watermarks which embed added information in every part of an image, only the complex parts of the image holds added information. Straight message insertion will simply encode every bit of information in the image. More complex encoding can be done to embed the message only in "noisy ‘areas of the image that will attract less attention [3]. The least significant bit (LSB) insertion method [4-12] is probably the most well known image steganography technique. The main advantage of this method is that human eye is not able to notice the change; however unfortunately, it is extremely vulnerable to attacks, such as image manipulation. JPEG image format due to its good characteristics (having both reasonable quality and small size) is the most common image format for web and local usages. JPEG uses discrete cosine transform (DCT) to transform successive 8×8 pixel blocks of the image into 64 DCT coefficients. Here, LSBs of the quantized DCT coefficients are used as redundant bits. The modification of even a single DCT coefficient affects all 64 image pixels. As the modifications happen in the frequency domain rather than spatial domain, there is no visual attack against it. Recently, several steganographic techniques for data hiding in JPEGs have been developed [13-15]. All these techniques manipulate the quantized DCT coefficients to embed the hidden message.

The theory of substitution technique is that simply replacing either a bit or a few bits in each sample will not be noticeable to the human eye or ear depending on the type of file. This method has high embedding capacity but it is the least robust. The obvious advantage of the substitution technique is a very high capacity for hiding a message. Obviously, the capacity of substitution techniques is not comparable with the capacity of other more robust techniques like spread spectrum technique that is highly robust but has a negligible embedding capacity (4bps) [16].

1.2. Optimum Pixel Adjustment Procedure

The Optimal Pixel Adjustment Procedure (OPAP) reduces the distortion caused by the LSB substitution method. In OPAP method the pixel value is adjusted after the hiding of the secret data is done to improve the quality of the stego-image without disturbing the data hidden [17]. This procedures is simple, easy retrieval and improved image quality.

1.3. Inverted Pattern Approach (IP)

This inverted pattern (IP) LSB substitution approach uses the idea of processing secret messages prior to embedding. In this method each section of secret images is determined to be inverted or not inverted before it is embedded. In addition, the bits which are used to record the transformation are treated as secret keys or extra data to be re-embedded [18].

1.4. Hiding Streams of 1s and 0s

The usual steganographic methods fetch few bits from the secret data to be embedded. But this method fetches the 1s or 0s present consecutively for hiding. This is an innovative steganographic method where the data to be hidden is converted to binary. The number of 1s and 0s are counted and stored in the pixels of the cover image in this method. The number of 1s is stored in the odd columns of the pixel and the number of 0s is stored in the even columns [19].

1.5. Pixel Value Differencing (PVD)

Pixel Value Differencing is able to provide a high quality stego image in spite of the high capacity of the concealed information. That is, the number of insertion bits is dependent on whether the pixel is an edge area or smooth area. In edge area the difference between the adjacent pixels is more, whereas in smooth area it is less. While human perception is less sensitive to subtle changes in edge areas of a pixel, it is more sensitive to changes in the smooth areas. This method hides the data in the target pixel by finding the characteristics of four pixels surrounding it [20].

1.6. The PVD Method

This method also uses the concept of hiding the data using the difference between the pixel values. Unlike the previous method, this method hides the data in the difference between two adjacent pixel values. This method gives the stego images of better quality than the traditional method while maintaining a high embedding capacity [19].

1.7. The Mod Method

In this method embedding is done by subtracting any remainder obtained by dividing with 10 and adding the data to be hidden. This is demonstrated by let the pixel be ‘p’ and data be less than 10 say‘d’ then new pixel formed is

$$p_1=p- \text{remainder } (p/10) +d \quad (1)$$

Similarly mod100 method divides the pixel by 100, remainder obtained is subtracted and the data is added to it to get the new pixel. The data hidden will simply be equal to the remainder obtained by dividing the new pixel by 10 or 100 accordingly. This is a method where the data is hidden in the difference between the adjacent pixels, so that mere extraction of few LSB bits will never give the data hidden. Also there is the key file without which extraction of data becomes impossible [19]. Besides there are different methods such as 2D block DCT [21-22], without parity bit [23], spread spectrum [24-26], genetic and wavelet [27], edge detection [7, 28-30], biometric [31] already researched and implemented. A lot of survey [32-40] on image stegonography has done by researchers.

III. MATERIALS AND METHODS

As we know in samples LSBs are more suspicious, thus embedding in the bits other than LSBs could be helpful to increase the robustness. Furthermore, discovering which samples are modified should be uncharted. To reach to the level of ambiguity, the algorithm will not use a predefined procedure to modify the samples but will decide, according to the environment, in this case the host file; as such it will modify indistinct samples of image files, depending on their values and bits status. Thus, some of the samples which algorithm determines they are suitable for modifying will modify and other samples may not change. This ambiguity in selecting samples will thus increase security and robustness of the proposed system. So embedding the bits in deeper layer depending on the environment of the cover image and alter other bit when required will increase the robustness of image steganography and also decrease the alteration complexity. In addition, when not possible in any sample it will ignore them.

3.1. The Embedding Process

In this dynamic technique of substitution based image steganography, first the number of 1 bits of the pixel in cover image is count. If this value is greater than or equal to one and less than the total number of bits in the sample bits then the host is a candidate for substitution. Number of message bits, use as key value. Then number of 1 in sample and secret key value are add and then mod by 8. This value is the position substitution. Now the bit value of that position and the message bit is X-ORed and if this result is 0 then no need to substitution. But if this result is 1, then substitute the bit positioned by message bit and adjust a near bit that equals to the message bit by altering that bit to keep the number of 1’s are same as was in the host. The process of message embedding through stego-system encoder is shown in Figure 4. To embed the message into the cover image follows the step below:

Step 1: Covert the message into bits. Here length of message bits used as key.
Step 2: Count the number of 1’s in the sample host image, n.

Step 3: If n is greater than or equal to one and less than number of all the bits of the stego sample, then it is a candidate for bit embedding otherwise ignore the sample
Step 4: Calculate p = (n+S_k) mod 8, here S_k means the secret key and 8 is the number of bits in one pixel.
Step 5: Calculate r=h_p xor m_b (h_p= bit of the host sample in position p and m_b is the message bit to embed)
Step 6: If r is equal to zero then need not modify and adjust the bit of the sample otherwise change h_p by m_b and adjust a near bit that is equal tomb by altering it.
Step7: Repeat the steps 2 to 6 until all the bits of the message is completed to embed.

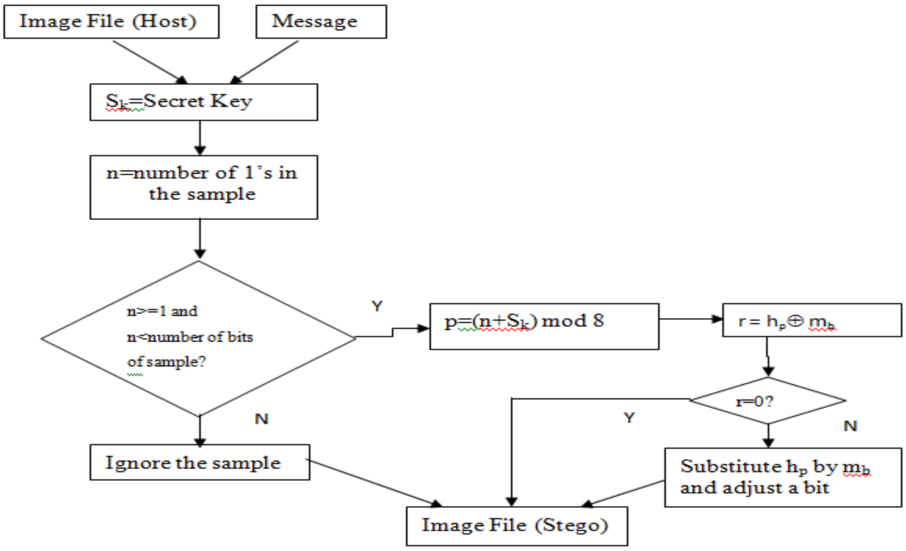


Figure 4: Message embedding process

Message Extraction Process

To get the message from the stego-image, first count the number of 1 bit in the stego-image. If this value is greater than or equal to one and less than the total number of bits in the sample bits then the stego is a candidate for getting the embedding bit of the message otherwise escape the sample. The position of the bit is calculated by (counted value + secret key) mod 8 in the stego-image that is the embedding message bit.

Step 1: Count the number of 1's from the stego-image, n
Step 2: If n is greater than or equal to one and less than number of all the bits of the stego sample, then it is a candidate for bit extraction otherwise ignore the sample
Step 3: Calculate p = (n+ S_k) mod 8, here S_k is the Secret key and 8 is the number of bits in one pixel.
Step 4: Extract the bit S_p (S_p = bit of the stego sample in position p)
Step 5: Repeat the steps 1 to 4 until all the bits (equal to S_k) of the message is extracted
The process of message extract is shown by the flowchart in the Figure 5.

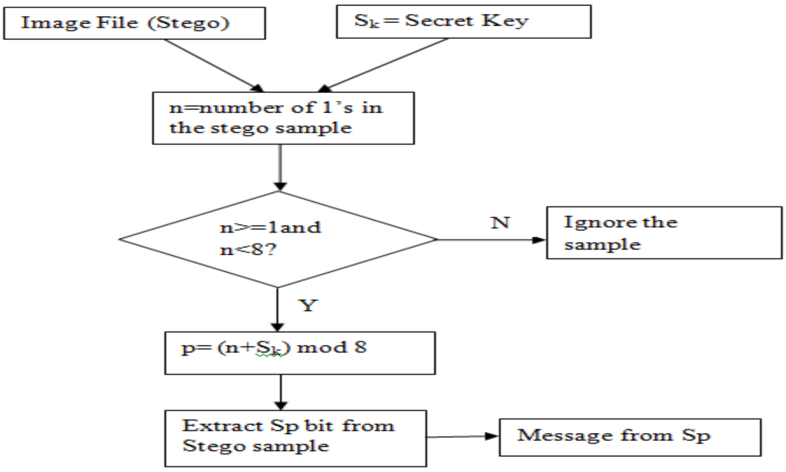


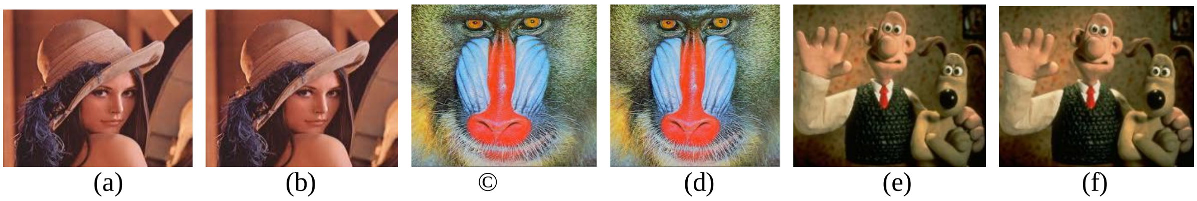
Figure 5: Message extraction process

IV. RESULT AND DISCUSSION

We have implemented the proposed method by using MATLAB R2007b. First we took three cover images (namely Lena, Baboon, Cartoon) of size 256X256 and a message. Then message is converted in to bits and this number of bits acts as the secret key. The images are also converted into series of bits and message bits are inserted in to this cover images according to our method (Dynamic substitution based Image steganography). After embedding the message into the cover images, we have got the stego-images that are closely similar with cover images shown in Figure 6.

Embedded Message: Daffodil University is one of the best private universities in Bangladesh.

Extraction message from Stego-images: Daffodil University is one of the best private universities in Bangladesh.



(a) (b) © (d) (e) (f)

Figure 6: Cover image and stego-image (a) Cover image: Lena (b) Stego-image: Lena (c) Cover image: Baboon (d) Stego-image: Baboon (e) Cover image: Cartoon (f) Stego-image: Cartoon

4.1. Comparison between LSB Method and Proposed Method

In LSB having low robustness against attacks which try to reveal the hidden message. But in our proposed method it is difficult to attack, because message bits are not inserted in to the fixed position. It is low robustness against distortions with high average power in LSB. But in our method we adjust pixels bits after insert the message bits that is high robust against distortions. Secret key generation process is easy and provides additional security of the stego-system.

4.2. PSNR Calculation

PSNR is one of metrics to determine the degradation in the embedded image with respect to the host image. Values over 36dB in PSNR are acceptable in terms of degradation, which means no significant degradation is observed by human eye.

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codec's (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codec's, PSNR is an *approximation* to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content.

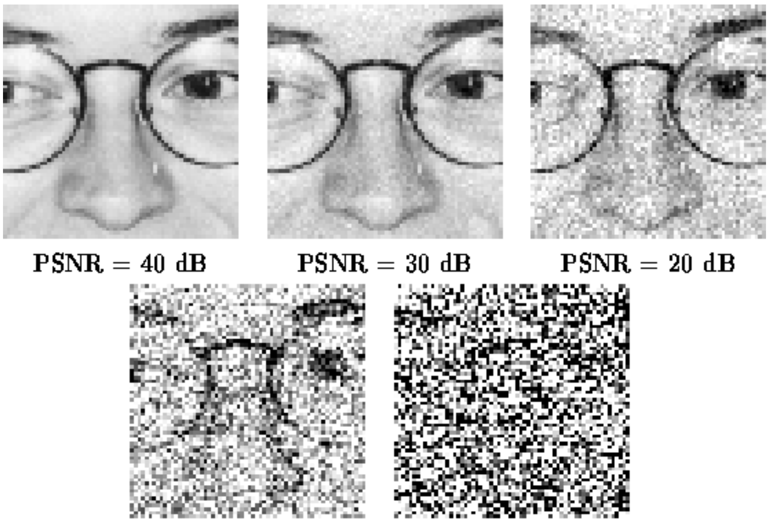
As a performance measurement for image distortion, the well-known Peak-Signal-to-Noise Ratio (PSNR) which is classified under the difference distortion metrics can be applied on the stego images. It is defined as:

$$PNSR = 10\log 10\,\left(\frac{C_{max^2}}{MSE}\right) \qquad (2)$$

Where *MSE* denotes Mean Square Error which is given as:

$$MSE=\frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy}-C_{xy})^2 \qquad (3)$$

Where *x* and *y* are the image co-ordinates, *M* and *N* are the dimensions of the image, S_{xy} is the generated stego-image and C_{xy} is the cover image. Also 2 C_{max}^{2} hold the maximum value in the image. PSNR values falling below 30dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego-image should strive for 40dB and above. MSE and PSNR figures provided in this thesis were calculated after quantization (i.e. after converting floating-point pixel values to integer), but before clipping of the intensity range.



PSNR = 40 dB PSNR = 30 dB PSNR = 20 dB

PSNR = 10 dB PSNR = 0 dB

Figure 5: Illustration of the PSNR measure

Table I represents the PSNR comparison of LSB substitution and our method using cover image Lena, Baboon and Cartoon.

Table I: Comparison of image steganography algorithms

Cover Image	LSB	Dynamic Substitution
Lena	44.0216	44.7638
Baboon	37.8642	38.7295
Cartoon	43.9901	44.7354

V. CONCLUSION

Many techniques are used to hide data in various formats in steganography. The most widely used mechanism on account of its simplicity is the least significant bit. Least significant bit or its variants are normally used to hide data in a digital image. The other bits may be used but it is highly likely that image would be distorted. However, in the present the bits used were not in fixed position. The LSB technique used in the present study is simple; it generally causes noticeable distortion when the number of embedded bits for each pixel exceeds three. In Optimal Pixel Adjustment Procedure (OPAP) method the pixel value is adjusted after the hiding of the secret data is done to improve the quality of the stego image without disturbing the data hidden. In inverted pattern (IP) method each section of secret images is determined to be inverted or not inverted before it is embedded. The secret key is generated automatically after embedding. The usual steganographic methods fetch few bits from the secret data to be embedded. But this method fetches the 1s or 0s present consecutively for hiding. This is an innovative steganographic method where the data to be hidden is converted to binary. The number of 1s and 0s are counted and stored in the pixels of the cover image in this method. The number of 1s is stored in the odd columns of the pixel and the number of 0s is stored in the even columns. In this method embedding is done by subtracting any remainder obtained by dividing with 10 and adding the data to be hidden. Similarly mod100 method divides the pixel by 100, remainder obtained is subtracted and the data is added to it to get the new pixel. The data hidden will simply be equal to the remainder obtained by dividing the new pixel by 10 or 100 accordingly. Message capacity and stego-image quality are two important criteria in evaluating a steganogarphic method. This new approach of dynamic substitution based image steganography has high robustness against attacks which try to reveal the hidden message and low robustness against distortions with high average power. The proposed method will embed the message bits in the deeper layers of samples and alter a bit near the substitute bit to decrease the error and if not possible then ignore them and improved security, reliability, and efficiency. So, using the proposed method, message bits could be embedded into vague and deeper layer depending on the environment of the host sample robustness. Our future work will cover against all kinds of intentional and unintentional attacks to increase the robustness of the image steganography. Our experimental results have shown that the proposed method provides good image quality and large message capacity as well as increase in the system immunity. It is very sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image will destroy the message. Our future work will be recovering it.

REFERENCES

[1] M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, *International Journal of Modelling and Simulation, 18(2),* 1998, 112-116.

[2] H. Wang, S. Wang, Cyber warfare: Steganography vs. Steganalysis, *Communications of the ACM, 47(10),* 2004

[3] C. Stanley, *Pairs of Values and the Chi-squared Attack*, Master's thesis, Department of Mathematics, Iowa State University, 2005

[4] M. A. F. Al-Husainy, Message Segmentation to Enhance the Security of LSB Image Steganography, *International Journal of Advanced Computer Science and Applications, 3(3),* 2012, 57-62

[5] N. Santoshi, B. L. Rao, A Secure and Lossless Adaptive Image Steganography with Mod-4 LSB Replacement Methods Using Image Contrast, *International Journal of Scientific & Engineering Research, 3(8),* 2012, 1-9

[6] M. Kavitha, K. Kadam, A. Koshti, P. Dungha, Steganography Using Least Signicant Bit Algorithm, *International Journal of Engineering Research and Applications (IJERA), 2(3),* 2012, 338-341

[7] N. Jain, S. Meshram, S. Dubey, Image Steganography Using LSB and Edge – Detection Technique, *International Journal of Soft Computing and Engineering (IJSCE), 2(3)*, 2012, 217-222

[8] S. Singh, G. Agarwal, Use of image to secure text message with the help of LSB replacement, *International Journal of Applied Engineering Research, 1(1),* 2010, 200-205

[9] R. Kaur, B. Singh, I. Singh, A Comparative Study of Combination of Different Bit Positions in Image Steganography, *International Journal of Modern Engineering Research (IJMER), 2(5),* 2012, 3835-3840

[10] B. Karthikeyan, S. Ramakrishnan, V. Vaithiyanathan, S. Sruti, M. Gomathymeenakshi, An Improved Steganographic Technique Using LSB Replacement on a Scanned Path Image, *International Journal of Network Security, 15(1),* 2013, 314-318

[11] V. Tyagi, A. Kumar, R. Patel, S. Tyagi, S. S. Gangwar, Image Steganography using Least Significant Bit with Cryptography, *Journal of Global Research in Computer Science, 3(3),* 2012, 53-55

[12] N. Tiwari, M. Shandilya, Evaluation of Various LSB based Methods of Image Steganography on GIF File Format, *International Journal of Computer Applications, 6(2), 2010*, 1-4

[13] J. Fridrich, M. Goljan, D. Hogea, Attacking the Out Guess, Proc. ACM Workshop Multimedia and Security2002, ACM Press

[14] A. Westfeld, High Capacity Despite Better Steganalysis (F5–ASteganographic Algorithm), *Information Hiding. 4th International Workshop on Information hiding,* New York, 2001, 289–302

[15] N. Provos, Defending Against Statistical Steganalysis, Proc.10th USENIX Security Symposium, Washington, 2001

[16] S. K. Pal, P. K. Saxena, S. K. Mutto, The Future of Audio Steganography, *Pacific Rim Workshop on Digital Steganography*, Japan, 2002

[17] C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, *Journal of Pattern Recognition, 37(3)*, 2004, 469–474

[18] C. H. Yang, Inverted pattern approach to improve image quality of information hiding by LSB substitution, *Journal of Pattern Recognition, 41*, 2008, 2674–2683

[19] R. Amirtharajan, R. Akila, P. Deepikachowdavarapu, A Comparative Analysis of Image Steganography, *International Journal of Computer Applications, 2(3),* 2010, 41-47

[20] Y. R. Park, H. H. Kang, S. U. Shin, K. R. Kwon, An Image Steganography Using Pixel Characteristics, CIS 2005, Part II, Springer-Verlag Berlin Heidelberg LNAI 3802, 2005, 581– 588

[21] K. B. S. Kumar, K. B. Raja, R. K. Chhotaray, S. Pattnaik, Steganography Based on Payload Transformation, *International Journal of Computer Science, 8(2)*, 2011, 241-248

[22] M. Singh, R. Sharma, D. Garg, A New Purposed Issue for Secure Image Steganography Technique Based On 2-D Block DCT and DCT, *International Journal of Advanced Research in Computer Science and Software Engineering, 2(7)*, 2012, 29-34

[23] C. N. Yang, J. Ouyang, L. Harn, Steganography and authentication in image sharing without parity bits, *Journal of Optics Communications, 285*, 2012, 1725–1735

[24] L. M. Marvel, C. G. Boncelet, C. T. Retter, Spread Spectrum Image Steganography, *IEEE Transactions on Image Processing, 8(8)*, 1999, 1075-1083

[25] S. Goyat, A Novel Technique Used For Image Steganography Based On Frequency Domain, *International Journal of Engineering Research & Technology (IJERT), 1(7),* 2012, 1-15

[26] G. S. Sravanthi, B.S. Devi, S. M. Riyazoddin, M. J. Reddy, A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method, *Global Journal of Computer Science and Technology Graphics & Vision, 12(15),* Version 1.0, 2012

[27] E. Ghasemi, J. Shanbehzadeh, N. Fassihi, High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm, *Proc. of International Multi Conference of Engineers and Computer Scientists*, March 16-18 2011, Hong Kong

[28] S. Arora, S. Anand, A Proposed Method for Image Steganography Using Edge Detection, *International Journal of Emerging Technology and Advanced Engineering, 3(2)*, 2013, 296-297

[29] A. A. Ali, A. H. S. Saad, New Image Steganography Method by Matching Secret Message with pixels of Cover Image (SMM), *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), 3(2*), 2013, 1-10

[30] A. M. A. Shatnawi, A New Method in Image Steganography with Improved Image Quality, *Journal of Applied Mathematical Sciences, 6(79)*, 2012, 3907 – 3915

[31] A.Cheddad, J. Condell, K. Curran, P. M. Kevitt, Biometric Inspired Digital Image Steganography, *15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems*, 2008

[32] A. Cheddad, J. Condell, K. Curran, P. M. Kevitt, Digital image steganography: Survey and analysis of current methods, Journal *of Signal Processing, 90*, 2010, 727–752

[33] G. Kaur, A. Kochhar, Transform Domain Analysis of Image Steganography, *International Journal for Science and Emerging Technologies with Latest Trends" 6(1)*, 2013, 29-37

[34] J. Kaur, S. Kumar, Study and Analysis of Various Image Steganography Techniques, *International Journal of Computer Science and Technology, 2(3)*, 2011, 535-539

[35] B. Li, J. He, J. Huang, Y. Q. Shi, A Survey on Image Steganography and Steganalysis, *Journal of Information Hiding and Multimedia Signal Processing , 2(2)*, 2011, 142-172

[36] M. Kumari, A. Khare, P. Khare, JPEG Compression Steganography & Cryptography Using Image-Adaptation Technique, *Journal of Advances Information Technology, 1(3)*, 2010, 141-145

[37] N. Hamid, A. Yahya, R. B. Ahmad, O. M. Al-Qershi, Image Steganography Techniques: An Overview, *International Journal of Computer Science and Security (IJCSS), 6(3)*, 2012, 168-179

[38] M. Kharrazi, H. T. Sencar, N. Memon, Performance study of common image steganography and steganalysis techniques, *Journal of Electronic Imaging 15(4), 2006*

[39] M. S. Prasad, S. Naganjaneyulu, G. Krishna, C. Nagaraju, A Novel Information Hiding Technique for Security by Image Steganography, *Journal of Theoretical and Applied Information Technology, 8(1),* 2009, 35-39

[40] N. Tiwari, M. Shandilya, Evaluation of Various LSB based Methods of Image Steganography on GIF File Format, *International Journal of Computer Applications, 6(2), 2010*, 1-4