Asian Journal of Information Technology 12 (10): 334-341, 2013
ISSN: 1682-3915
© Medwell Journals, 2013

Providing a Better Protection During Exchange of Critical Data Based on Information Hiding Mechanism

[1]V. Muneeswaran and [2]S. Subramanian
[1]Anna University, Chennai, Tamilnadu, India
[2]Coimbatore Institute of Engineering Technology, Coimbatore, Tamilnadu, India

Abstract: With the rapid advances in communication technology, most of the trusted data exchange happens electronically through various mediums such as Short Messaging Service (SMS), Multimedia Messaging Service (MMS) and electronic mail (e-mail) in the form of text, image, audio and video. For secure data exchange steganography can be employed rather than cryptography. Steganography is an ancient art of hiding confidential information in unsuspected objects like text, image, audio, video and Deoxyribonucleic Acid (DNA). It must not be confused with cryptography where it transforms the confidential data into unintelligible one. It does not give a meaning to a person who intercepts it. Digital technology gives us new ways to apply steganographic techniques including one of the most interesting practices of hiding information in digital images. An image can have more information than what researchers see with the Human Visual System (HVS) hence they can convey more than a 1000 words. The steganography technique that is provides a better protection to a data in transmission while compared to other techniques. It provides a high information hiding capacity and successfully controls the distortion of the stego image. This study presents a new way of providing confidential information in a secure manner.

Key words: Trusted data, protection, information hiding, cryptography, image, least significant bit, exchange

INTRODUCTION

With the digitalization of data and networking of communication, the exchange of secret data within the sender and receiver in the network will be a crucial one. Sending secret information over public networks is insecure (Chang *et al*., 2008). In essence, the internet is an open channel and the security problems such as interception, modification, confidentiality, authentication and others are very real. Several approaches have been proposed to make communication via the Internet secure (Chang *et al*., 2007).

To the best of the knowledge, all the most popular forms of security protection heavily rely on encryption which refers to the process of encoding secret information in such a way that only the person with the right key can successfully decode it. However, encryption leaves obviously noticeable marks on the eavesdroppers' attention. Another way to solve this problem is to hide the secret information behind some cover such as a digital images or a sound clip so that it draws no special attention. This technique of information security called steganography is applicable to many situations in which invisible communications take place (Tseng and Chang, 2004). Steganography is different from classical encryption which conceals the contents of secret messages.

Steganography has various useful applications such as human right organizations (Anderson and Petitcolas, 1998), smart identity cards where individual details are embedded in their photographs, data integrity by embedding checksum and secure transmission of medical, critical or trusted data. Now a days, all medical related data's can be stored in the form of digital in most of the hospitals. The data's are stored in the form of text, image, audio and video. But most of the information or nearly 80% of data can be stored as text information, only 10-20% of work can be either the form of image, video or audio.

These types of data can be transmitted over the internet if any further clarification from the expert doctors. During the transmission process if any hacker who wants to hack the information he easily got the message because it is available as it is. This type of information will store in the server which is located in the hospital. So, anybody who knows to access the server can easily outsource the medical records. With the development and generality of the network technique, the transmission of digitized

Corresponding Author: V. Muneeswaran, Anna University, Chennai, Tamilnadu, India

medical information has become very convenient. The development of the internet network makes the way of medical care have great transitions too fast now. The advantage of using the internet network in medical science, regardless of preventing medical research, support clinical diagnosis, unusual incident perceive in time and it can help the patient to take medicine safely. However, the hackers can easily get the information through internet to duplicate or to revise it easily. As a result, this issue is working paying attention such as the medical security and copyright protection. Therefore, the information hiding techniques are developed for protection of medical information and copyright (Lou *et al*., 2008).

Imperceptibility, robustness, capacity and security are the four basic requirements for data hiding techniques. It is not an easy research to meet all the above four requirement in a data hiding scheme. Use trade off mechanism between them and choose a best suitable one. For example embedding a large amount of data into a picture can cause a noticeable research of art. On the other hand to improve the imperceptibility, the capacity of the data will also condense. Therefore, depending upon the application users need to select the appropriate the data hiding scheme.

Currently there are two major types of data hiding techniques in the real world environment. One is Spatial Domain (SD) and the other one is Transform Domain (TD). Least Significant Bit insertion (LSB) (Walton, 1995), Vector Quantization (VQ) (Chen *et al*., 1998), patchwork (Fridrich *et al*., 2002) and texture block are some examples of spatial domain techniques. This technique embeds the data directly by modifying the pixel values of the target pictures. The lower computational complexity and higher embedding capacity are the main advantages of this technique. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) (Tian, 2002) are some examples of transform domain techniques. In this technique the data can be embed by modulating the coefficients of pixel value. Steganography has become popular because of two reasons:

- Hiding of copyright and serial number information
- Restriction of availability of encryption services has motivated people to study methods for embedding messages

With advancement in digital communication technology, growth of computer power and storage, the difficulties in ensuring individuals privacy become increasingly challenging. The degrees to which individuals appreciate privacy differ from one person to another.

Various methods (Encryption, Steganography and Password protection) have been investigated and developed to protect personal privacy. Encryption lends itself to noise and is generally observed while steganography is not observable.

Steganography is different from cryptography as encryption provides a different level of security to a data. One of the most common uses of modern steganography in the digital world computers is to hide information from one file in the contents of another file.

The common approaches include LSB insertion, masking, filtering and transform techniques. The stego-image seems identical to the cover image even though the cover image is combined with the message (Amin *et al*., 2003). Cryptography combined with steganography will provide an additional layer of security (Johnson and Jajodia, 1998).

LITERATURE REVIEW

For decades people strove to develop innovative methods for secret communication. Three techniques are interlinked, steganography, watermarking and cryptography. The first two are quite difficult to tease apart especially for those coming from different disciplines. Drawing a line between these techniques is both arbitrary and confusing (Wayner, 2002). Therefore, it is necessary to discuss briefly these techniques before a thorough review is provided. Figure 1 and Table 1 may eradicate such confusion.

In the real world, the security solutions are providing with cryptography and information hiding mechanism. The cryptography mechanism further classified as public key cryptography and private key cryptography depending on the usage of key in sender as well as receiver side. Similarly, the information hiding mechanism can further divided into watermarking and steganography, respectively. Information hiding generally relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness that is it should be impossible to remove a

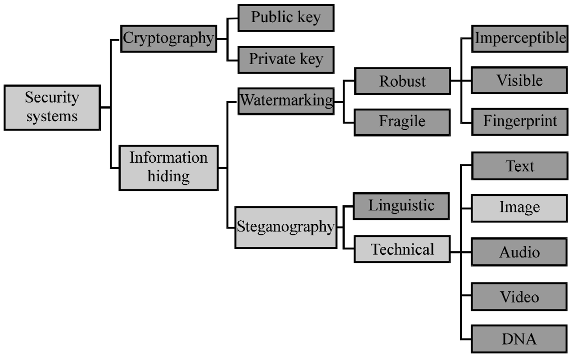

Fig. 1: Information hiding techniques

Table 1: Comparison of steganography, watermarking and cryptography

Criterion/Method	Steganography	Watermarking	Cryptography
Carrier	Any digital media	Mostly image/audio files	Usually text based with some extensions to image files
Secret data	Payload	Watermark	Plain text
	No changes to the structure		Changes the structure
Key	Optional		Necessary
Input files	At least two unless in self-embedding		One
Detection	Blind	Usually informative i.e., original cover or watermark is needed for recovery	Blind
Authentication	Full retrieval of data	Usually achieved by cross correlation	Full retrieval of data
Objective	Secrete communication	Copyright preserving	Data protection
Result	Stego-file	Watermarked-file	Cipher-text
Concern	Delectability/Capacity	Robustness	Robustness
Type of attacks	Steganalysis	Image processing	Cryptanalysis
Visibility	Never	Sometimes	Always
Fails when	It is detected	It is removed/replaced	De-ciphered
Relation to cover	Not necessarily related to the cover. The message is more important than the cover	Usually becomes an attribute of the cover image. The cover is more important than the message	Not applicable
Flexibility	Free to choose any suitable cover	Cover choice is restricted	Not applicable
History	Very ancient except its digital version	Modern era	Modern era

watermark without degrading the data object's quality. Steganography on the other hand, strives for high security and capacity which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it (Provos and Honeyman, 2003).

The main driving force in watermarking is concern over protecting copyright as audio, video and other works as they become available in a digital format. It is feared that the ease with which perfect copies can be made will lead to large-scale unauthorized copying which will undermine the music, film, book and software publishing industries. The watermarking is subdivided into two major categories such as robust watermarking and fragile watermarking. There has therefore been significant recent research into imperceptible, visible and fingerprinting watermarking for hidden copyright information's and hidden serial numbers or a set of characteristics that tend to distinguish an object from other similar objects the idea is that the latter can be used to detect copyright violators and the former to prosecute them (Fard *et al.*, 2006).

The research presented here revolves around steganography in digital images and does not discuss other types of steganography such as linguistic and technical. Table 1 summarizes the differences and similarities between steganography, watermarking and cryptography. Figure 2 demonstrates the main aims of steganography and watermarking which are the exact extraction of the hidden data for steganography and the detection for watermarking. Figure 2 also shows the attackers' main objectives, detection and destruction for steganography and watermarking, respectively. Figure 2 shows (top) aim of the embedder and (bottom) the aim of the attackers.

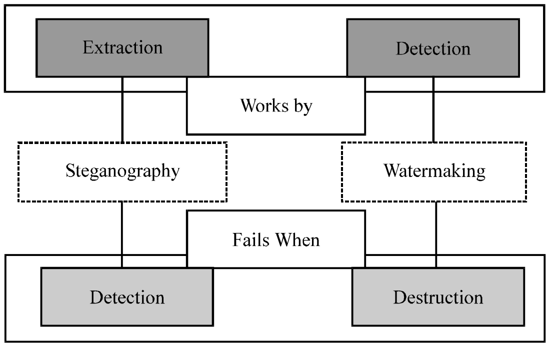

Fig. 2: Steganography vs. watermarking

Steganography methods: This study attempts to give an overview of the most important steganographic techniques in digital images. The most popular image formats, non-scientific images used on the internet are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG) and to a lesser extent-Portable Network Graphics (PNG). Most of the techniques developed aimed to exploit the structures of these particular formats. There are some exceptions in the literature that use the Bitmap format (BMP) due to its simple data structure.

The process of embedding is defined as follows a graphical representation is shown in Fig. 3. Let C denote the cover carrier, i.e., image A, M the data to hide, $\hat{M}$ the extracted file, g_k the steganographic function and C' the stego-image. Let K represent an optional key a seed used to encrypt the message or to generate a Pseudo Random (PR) noise which can be set to {Ø}, the null set for simplicity and let M be the message to communicate, image B. E_m is an acronym for embedding and E_x is an acronym for extraction. Therefore, a complete steganographic system would be:

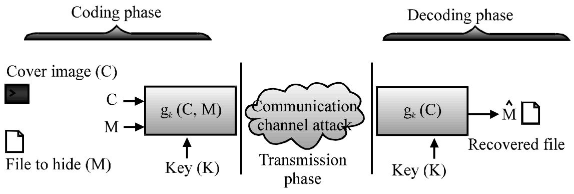

Fig. 3: Communication-theoretical view of a generic embedding process

$$\text{Em: } C \oplus k \oplus M \rightarrow C' \tag{1}$$

$$E_x\left(E_m\left(c, k, m\right)\right) \approx m, \forall c \in C, k \in K, m \in M \tag{2}$$

Related works: The main steganographic methods such as:

- Spatial domain techniques which generally use a direct LSB replacement method
- Frequency domain based methods such as Discrete Cosine Transform (DCT), Fourier Transform (FT) and Discrete Wavelet Transform (DWT)
- Perceptual Masking (PM) or Adaptive Steganography (AS)

The categorization of steganographic algorithms into the three categories, namely, spatial domain, frequency domain and adaptive methods is unique to this research and there is no claim that it is a standard categorization. Adaptive methods can either be applied in the spatial or frequency domains and are thus regarded as special cases. Image-format based steganography techniques are not included here as they are naive implementations and extremely prone to detection.

LSB Method: For a gray scale image LSB requires 8 pixel values to store one byte information. However, the amount of information being embedded is reduced for a gray scale image in comparison to color image. The LSB algorithm researchs by taking each byte of a 24 bit image and store three bits in each pixel. The resulting stego-image will look identical to the cover image (Tseng and Chang, 2004).

Masking and filtering is restricted to 24 bit and gray scale images in a manner similar to study water marks. Masking is more robust than LSB insertion with respect to compression, cropping and some image processing.

DCT Method: Steganography based on DCT, JPEG compression, follows steps as shown in Fig. 4. Most of the techniques here use JPEG images within which to embed the data. JPEG compression uses the DCT to transform successive sub-image blocks, 8×8 pixels, into 64 DCT coefficients. Data is inserted into these coefficients' insignificant bits however, altering any single coefficient would affect the entire 64 block pixels (Fard *et al*., 2006). As the change is operating on the frequency domain instead of the spatial domain there will be less visible change in the cover image given those coefficients are handled with care (HAshad *et al*., 2005).

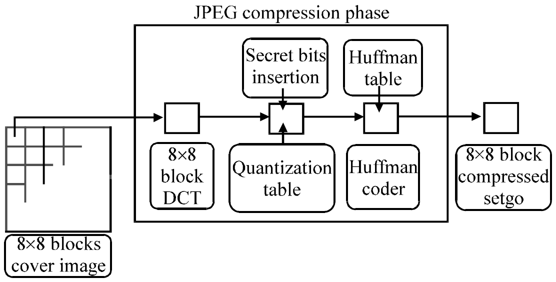

Fig. 4: Embedding data in frequency domain

DFT/FFT Method: According to Raja *et al*. (2005), Fast Fourier Transform (FFT), methods introduce round off errors thus are not suitable for hidden communication. However, Johnson and Jajodia (Tseng and Chang, 2004) included these methods among the used transformations in steganography and another researcher utilized the 2D Discrete Fourier Transform (DFT) to generate Fourier based steganography in movies (Sallee, 2003).

Adaptive steganography: Adaptive steganography is a special case of the two former methods. It is also known as statistics-aware embedding (Sallee, 2003), "Masking" or "Model-Based" (Tseng and Chang, 2004). This method takes statistical global features of the image before attempting to interact with its LSB/DCT coefficients. The statistics will dictate where to make the changes. It is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local, standard deviation. The latter is meant to avoid areas of uniform color, smooth areas. This behaviour makes adaptive steganography seek images with existing or deliberately added noise and images that demonstrate color complexity.

Difference Value Method: The hiding capacity depends on the Difference Value Method (Provos and Honeyman, 2003). The approach differs from the earlier ones as it changes the remainder slightly such that there is not much change in image quality. The image quality is tested first for minimum pixel value change and then for maximum pixel value change. Dual Statistics Method is used for checking the security of data.

Ajay proposed (Channalli and Jadhav, 2009) a new scheme for steganography by proposing on-line hiding of data. The method though similar to image steganography offers more amount of security. The cover media was analyzed for text file, image, audio and video file. The pattern bits formed is the basis for generating the secret file. Integrity and accuracy is used as the performance metric in the approach. It is proved that the quality of the media also plays a vital role during hiding information.

Embedding Considering Adjacent Pixels algorithm (Franz *et al*., 2009) is analyzed and the potential problems are identified to result from differences between the single representations of the cover. The four adjacent pixels are calculated separately and it could be improved averaging the pixel component values. It is proved that the introduction of outlier scans can improve the results. The method does not consider images that are obtained by a digital camera as cover set.

The model (Francia and Gomes, 2006) was enhanced by cleansing the cover media. A steganography obliterator algorithm is analyzed in the approach and the application handles an input file and applies masking and converts into another file for latter processing. The extensions could be extending LSB algorithm, GIF encoder revision also.

Embedding in 2LSB: There are two obvious ways to embed a payload by overwriting the least and second-least significant bits of a cover (Lou *et al*., 2008). For definiteness, researchers also describe the Standard LSB Embedding Method which is folklore to steganographers. The cover object has N bytes (more generally, words of some fixed bit length) and that the embedded payload is of proportionate length p with $0 \leq p \geq 1$ where the proportion is of the available capacity.

LSB approach works by embedding Np bits by selecting Np pixels and replacing the LSB of each pixel by the corresponding bit of the payload. Embedding in the Two LSB (2LSB) approach works by embedding 2Np bits in the cover by selecting Np pixels and replacing both of the two LSBs of each pixel with corresponding bits of the payload (Lou *et al*., 2008).

As an alternative method of using 2LSBs, bits can be embedded in the cover by selecting pixels and replacing only the second-LSBs of each pixel with a corresponding bits of the payload then repeating with a new selection of pixels of which only the LSB is used. Therefore, changes occur in the least and second-LSB planes independently (Lou *et al*., 2008). The 2LSB Embedding Method carries twice the payload of plain LSB Embedding Method.

PROPOSED TECHNIQUE

This study presents a new method of hiding data in cover image. The algorithms are designed to select pseudo random pixels from cover image for embedding data with a key that select the starting pixel from the cover image. The proposed scheme is shown in Fig. 5.

The main goal of steganography is to communicate securely in a completely undetectable manner. It is not to keep others from knowing hidden information. Essentially, the information hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity).

Least significant bit insertion is a simple approach to embed information in an image file. The simplest steganographic technique embed the bits of the message directly into least significant bit plane does not result in human-perceptible difference because the amplitude of the change is small. Digital images are typically stored in 24 bits files. A 24 bits image provides the more space for hiding information however it can be quite large. All the color variations for the pixels are derived from three primary colors such as red, green and blue. Each primary color is represented by 1 byte 24 bit images use 3 bytes per pixel to represent a color value. A white background would have the value FFFFFF: 100% red (FF), 100% green (FF), 100% blue (FF). Its decimal value is 255, 255, 255 and its binary value is 11111111, 11111111 and 11111111.

When considering an image in which to hide information, first consider the image as well as the palette. Obviously, an image with large areas of solid colors is a poor choice as variances created from the embedded

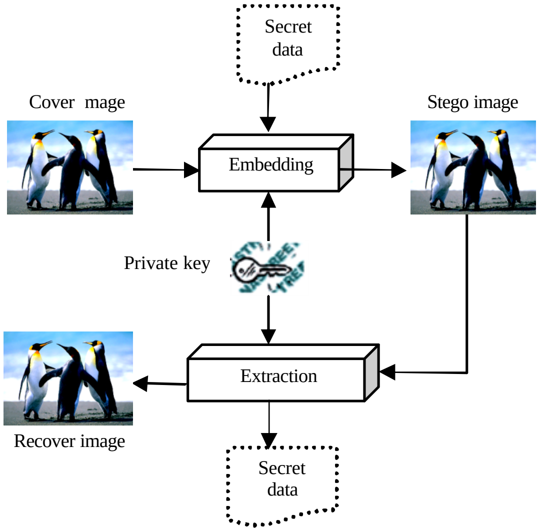

Fig. 5: Proposed data hiding technique

Table 2: Embedding process

The 3 bytes of Data "01001110 01100101 01110111" ASCII equivalent of "New"

Old pixel value			Old pixel value in binary			New pixel value in binary			New pixel value		
R	G	B	Red	Green	Blue	Red	Green	Blue	R	G	B
205	139	89	11001101	10001011	01011001	11001101	10001000	01011011	205	136	91
208	142	92	11010000	10001110	01011100	11010010	10001101	01011110	210	141	94
210	144	94	11010010	10010000	01011110	11010001	10010001	01011101	209	145	93
209	143	93	11010001	10001111	01011101	11010011	10001101	01011111	211	141	95
Before embedding process						After embedding process					

message will be noticeable in the solid areas. Once selected a cover image and then must decide on a technique to hide the information want to embed.

In this study, the selected cover image is a JPEG color image and the secret message is plain text. The embedding technique used here is 2LSB. The password which is act as a private key between sender and receiver will play a crucial role during the embedding process. Beaded on the password only, the cover image starting pixel is selected. The unique property for the pseudo random number is whenever a user generates a random number it follows a sequence. The user try to change its sequence use randomize property. A user generate a random number with a seed it always follow a sequence. With this property of pseudo random number the password is used as seed for generating the number so, always a unique sequence will be generated for each password.

The 3 bytes information is embedded in four pixels using 2LSB technique. The embedding process with the secret text New is illustrated in the following Table 2.

The total number of pixels required for embedding a 'N' byte of information is 4N/3 which is very much higher capacity of information compared with LSB technique. During extraction process the same password is used to pick the starting pixels of an image and extract the 2LSB in each pixel.

ANALYSIS AND TESTING

For analysis and testing, the various types of existing LSB algorithms were implemented in java. The comparison results are tabulated in the Table 3. For example in LSB algorithm, embedding a secret data of size N bytes which can be hidden in gray scale image needed 8 N pixels to store the data. It has very low security because anybody can easily retrieve the data when they collect each pixel last bit and group it by 8 bits. But the quality of a stego image is high because of only changes that made one bit only. Similarly the same type of LSB algorithm was used to embed a secret data in color image need maximum of 3 N pixels are required to store N byte of data. The selection of pixels type is sequential in the above LSB algorithm either gray or color image.

Table 3: Comparison of Lena and Bafoon image with different size of data values

		Pixel type		
Image name	Size of data	Red	Green	Blue
Bafoon	1 kB	43.08641	43.28450	43.20526
	2 kB	43.13076	43.11681	43.12279
Lena	1 kB	43.01715	43.09564	43.06277
	2 kB	43.14476	43.11681	43.14276

The performance measurement for an image distortion can be measured by the well known Peak Signal to Noise Ratio (PSNR) value which is classified under the difference distortion metrics can be applied to the stego images. It is defined as:

$$\text{PSNR} = 10\log_{10}\left(\frac{C_{\max}^{2}}{\text{MSE}}\right) \tag{3}$$

where, MSE denotes the Mean Square Error (MSE) which is given as:

$$\text{MSE} = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^{2} \tag{4}$$

Where:

x and y = The image coordinates
M and N = The dimensions of the image
S_{xy} = The reconstructed stego image
C_{xy} = The cover image
$C^{2}_{\max}$ = Holds the maximum value in the image for example:

$$C_{\max} \leq \begin{cases} 1 & \text{double-precision} \\ 255 & \text{8 bit} \end{cases}$$

Consider the Lena and Bafoon images for embedding secret information in 2LSB technique of sizes 1 and 2 kB, the PSNR vales are tabulated in Table 3. When compared with cover image the stego images much not have identify as much distortion with the human eyes.

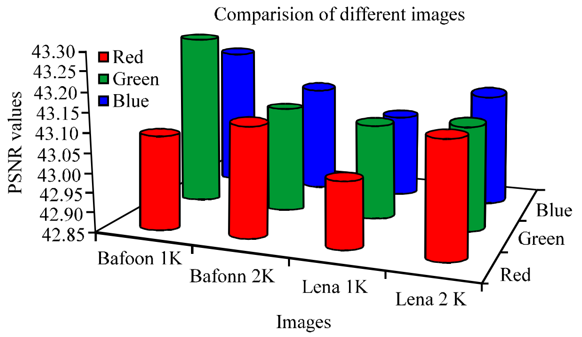

Fig. 5: Comparison of Lena and Bafoon Image

Table 4: Experimental results observations

Algorithm	LSB		2LSB	
Image type	Gray	Color	Gray	Color
Security	Low	Low	High	Very high
Time taken for embedding	More	More	Less	Very less
No. of pixels need	8 N	3 N	4 N	4 N/3
Imperceptibility /Stego-image quality	High	High	Low	High
Structural analysis	I/U/D	I/U/D	I/U/D	I/U/D
Pixel selection	Seq.	Seq.	Seq./Rnd	Seq./Rnd

N = No. of datum

This has been reflected in the PSNR values also. A high quality stego image should strive for a PSNR value of 40 dB and above. From the Fig. 6, embedding a double size of data in the cover image, the obtained PSNR values are nearly equal in each color components. It shows that even researchers embed a double size of the data the stego image is mostly look like as cover image, i.e, no much distortion is not obtainable in the stego images.

While embedding a 1 and 2 kB of data's in bafoon image the PSNR values of the red pixels are 43.08641 and 43.14076. By seeing these results, the difference between these two was 0.04435. Similarly researchers get the small difference in green as well as blue pixels also. The output stego image was not much disturbed because of the higher PSNR vales. By seeing with the eye, the stego image is look alike with the original cover image. Do not find the enough number of pixel distraction even increase the volume of embedding data.

From the analysis and testing with different types of images like grey, color and algorithm LSB, L2SB some of key points are observed and tabulated in Table 4. By seeing these results, the new algorithm L2SB have major advantage compare with the LSB algorithm in gray as well as color images. While considering the gray color images, the result of security is high, time taken for embedding a data is low and need only 4N pixels are needed.

Similarly with the results in color images, the security is very high and the time taken to embedding information is very less and it required only 4N/3 pixels and image quality is very high by comparing with gray color images. The selection of pixel as well as the embedding data the structural analysis may incremented or unchanged or decremented and the pixel selection either sequential or random mode in both type of the images.

CONCLUSION

This study has analysed with the various methods of steganographic technique like LSB and 2LSB. Compare with LSB, the 2LSB have more pay load of data with higher PSNR value. This will give better results in the stego image with the PSNR values. High PSNR is the cover image is very much similar to stego image and also it will give more information hiding in a color image compared to gray images. The focus was not just on the embedding strategy it gives more data hiding in images so that any eavesdropper cannot identify what is the information hidden behind an image. In future when strong information hiding mechanism will be needed; payload encryption, compression and embedding area selection strategies may be used.

REFERENCES

Amin, M.M., M. Salleh, S. Ibrahim, M.R. Katmin and M.Z.I. Shamsuddin, 2003. Information hiding using steganography. Proceedings of the 4th National Conference on Telecommunication Technology, January 14-15, 2003, Shah Alam, Malaysia, pp: 21-25.

Anderson, R.J. and F.A.P. Petitcolas, 1998. On the limits of steganography. IEEE J. Selected Areas Commun., 16: 474-481.

Chang, C.C., C.C. Lin, C.S. Tseng and W.L. Tai, 2007. Reversible hiding in DCT-based compressed images. Inform. Sci., 177: 2768-2786.

Chang, C.C., T.D. Kieu and Y.C. Chou, 2008. Reversible information hiding for VQ indices based on locally adaptive coding. J. Visual Commun. Image Representation, 20: 57-64.

Channalli, S. and A. Jadhav, 2009. Steganography an art of hiding data. Int. J. Comput. Sci. Eng., 3: 137-141.

Chen, T.S., C.C. Chang and M.S. Hwang, 1998. A virtual image cryptosystem based upon vector quantization. IEEE Trans. Image Process., 7: 1485-1488.

Fard, A.M., M.R. Akbarzadeh-T and F. Varasteh-A, 2006. A new genetic algorithm approach for secure JPEG steganography. Proceedings of IEEE International Conference on Engineering of Intelligent Systems, April 22-23, 2006, Islamabad, Pakistan, pp: 1-6.

Francia, G.A. and T.S. Gomez, 2006. Steganography obliterator: An attack on the least significant bits. Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, September 22-23, 2006, Georgia, USA., pp: 85-91.

Franz, E., S. Ronisch and R. Bartel, 2009. Improved embedding based on a set of cover images. Proceedings of the 11th ACM Workshop on Multimedia and Security, September 7-8, 2009, Princeton, NJ, USA., pp: 141-150.

Fridrich, J., M. Goljan and R. Du, 2002. Lossless data embedding-new paradigm in digital watermarking. EURASIP J. Applied Signal Process., 2002: 185-196.

Hashad, A.I., A.S. Madani and A.E.M.A. Wahdan, 2005. A robust steganography technique using discrete cosine transform insertion. Proceedings of ITI 3rd International Conference on Information and Communications Technology Enabling Technologies for the New Knowledge Society, December 5-6, 2005, Cairo, Egypt, pp: 255-264.

Johnson, N.F. and S. Jajodia, 1998. Exploring steganography: Seeing the unseen. Computer, 31: 26-34.

Lou, D.C., M.C. Hu and J.L. Liu, 2008. Multiple layer data hiding scheme for medical images. Comput. Standards Interfaces, 31: 329-335.

Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. IEEE Secur. Privacy, 1: 32-44.

Raja, K.B., C.R. Chowdary, K.R. Venugopal and L.M. Patnaik, 2005. A secure image steganography using LSB, DCT and compression techniques on raw images. Proceedings of 3rd International Conference on Intelligent Sensing and Information Processing, December 14-17, 2005, Bangalore, India, pp: 170-176.

Sallee, P., 2003. Model-based steganography. Proceedings of the 2nd International Workshop on Digital Watermarking, October 20-22, 2003, Seoul, Korea, pp: 254-260.

Tian, J., 2002. Wavelet-based reversible watermarking for authentication. Proceedings of the Security and Watermarking of Multimedia Contents IV, January 19, 2002, San Jose, CA., USA., pp: 679-690.

Tseng, H.W. and C.C. Chang, 2004. Steganography using JPEG-compressed images. Proceedings of the 4th International conference on Computer and Information Technology, September 14-16, 2004, Wuhan, China, pp: 12-17.

Walton, S., 1995. Image authentication for a slippery new age. Dr Dobb's J. Software Tools Prof. Programmer, 20: 18-27.

Wayner, P., 2002. Disappearing Cryptography: Information Hiding: Steganography and Watermarking. 2nd Edn., Morgan Kaufmann Publishers, San Francisco, CA, USA.