Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18, DOI: 10.14429/dsj.62.1436

REVIEW PAPER

Steganographic Techniques of Data Hiding using Digital Images

Babloo Saha and Shuchi Sharma

Institute for Systems Studies and Analyses, Delhi – 110 054, India
Jaipur Institute of Engineering and Technology, Jaipur – 303 101, India
E-mail: babloo.saha@gmail.com

ABSTRACT

Steganography is an art that involves communication of secret data in an appropriate carrier, e.g., image, audio, video or TCP/IP header file. Steganography's goal is to hide the very existence of embedded data so as not to arouse an eavesdropper's suspicion. For hiding secret data in digital images, large varieties of steganographic techniques are available, some are more complex than others, and all of them have their respective pros and cons. Steganography has various useful applications and the technique employed depends on the requirements of the application to be designed for. For instance. applications may require absolute invisibility of the secret data, larger secret data to be hidden or high degree of robustness of the carrier. This paper intends to give thorough understanding and evolution of different existing digital image steganography techniques of data hiding in spatial, transform and compression domains. It covers and integrates recent research work without going in to much detail of steganalysis, which is the art and science of defeating steganography.

Keywords: Digital image steganography, data hiding, cover-image, stego-image, redundant bits, least significant bit, most significant bit, reversible data hiding

1. INTRODUCTION

Steganography word is of Greek origin and essentially means concealed writing. Protection of the transmitted data from being intercepted or tampered has led to the development of various steganographic techniques. Steganography has been manifested long way back during the ancient Greek times. Greek tyrant Histiaeus in 499 BC shaved the head of his slave and wrote message on his scalp. After the hair grew back, slave was dispatched with the hidden message. Pliny the Elder explained how the milk of the *Thithymallus* plant dried to transparency when applied to paper but darkened to brown when subsequently heated, thus providing the way for hiding information. Giovanni Battista Porta described how to conceal a message within a hardboiled egg by writing on the shell with a special ink. In world war II long sentences of regular letters were used to disguise secret messages. With the tremendous advancement in digital signal processing, use of internet, computing power, steganography has gone digital. The data hiding process starts by identifying a cover image's redundant bits, i.e., those that can be modified without destroying its integrity. The embedding process then creates stego-image by replacing subset of these redundant bits with the bits of the message to be hidden. Generic steganography process is shown in Fig 1. In digital image steganography, the secret message is embedded within a digital image called cover-image. Cover-image carrying embedded secret data is referred as stego-image.

1.1. Applications of Steganography

Steganography can be used for wide range of applications such as, in defence organisations for safe circulation of secret data, in military and intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials. In medical imaging, patient's details are embedded within image providing protection of information and reducing transmission time and cost[1], in online voting system so as to make the online election secure and robust against a variety of fraudulent behaviours[2], for data hiding in countries where cryptography is prohibited, in improving mobile banking security[3], in tamper proofing so as to prevent or detect unauthorised modifications and other numerous applications

1.2 Features of Steganographic Techniques

Steganographic techniques have various features which characterises their strengths and weaknesses. Features include:

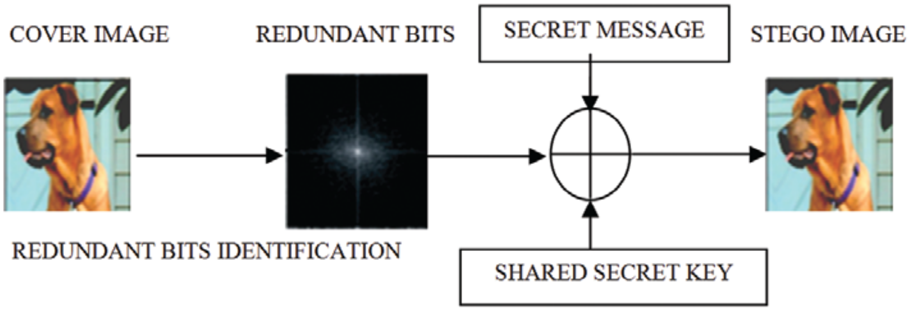

Figure 1. Generic steganography process.

Received 11 November 2011, online published 23 January 2012

Embedding capacity: It refers to the amount of data that can be inserted into the cover-media without deteriorating its integrity.

Perceptual transparency: It is necessary that to avoid suspicion the embedding should occur without significant degradation or loss of perceptual quality of the cover media.

Robustness: It refers to the ability of embedded data to remain intact if the stego-image undergoes various transformations such as scaling, rotation, cropping or compression.

Tamper resistance: It refers to the difficulty to alter or forge a message once it is embedded in a cover-media, such as replacing a copyright mark with the one claiming legal ownership.

Computational complexity: Computational complexity of steganography technique employed for encoding and decoding is another consideration and should be given importance.

1.3 Classifications of Steganographic Techniques

Classifications of steganographic techniques based on the types of cover files as shown in Fig 2. Almost all digital file formats can be used for steganography, however only those with a high degree of redundant bits are preferred. The larger size of audio and video files makes them less popular as compared to images. The term protocol steganography refers to embedding information within network protocols such as TCP/IP.

In Spatial domain, cover-image is first decomposed into bits planes and then least significant bit (LSB) of the bits planes are replaced with the secret data bits. Advantages are high embedding capacity, ease of implementation and imperceptibility of hidden data. The major drawback is its vulnerability to various simple statistical analysis methods. Frequency domain embedding techniques, which first transforms the cover-image into its frequency domain, secret data is then embedded in frequency coefficients. Advantages include higher level of robustness against simple statistical analysis. Unfortunately, it lacks high embedding. In compression domain, secret data is embedded into compression codes of the cover-image which is then sent to the receiver. It is of paramount importance where bandwidth requirement is a major concern.

2. SPATIAL DOMAIN-BASED STEGANOGRAPHIC TECHNIQUES

The most direct way to represent pixel's colour is by giving an ordered triplet of numbers: red (R), green (G), and blue (B) that comprises particular colour. The other way is to use a table known as palette to store the triplet, and put a reference into the table for each pixel. The spatial domain-based steganographic techniques use LSB algorithm for embedding/extraction of data as shown in Fig 3.

2.1 EzStego Data Hiding

EzStego data hiding scheme was given by Machado[4,5]. In this method palette is first sorted by luminance to minimize the perceptual distance between consecutive colours. EzStego then embeds the secret data into the LSB of the indices pointing to the palette colours. This approach works quite well in gray scale images and may work well in images with related colours. The major drawback is, since luminance is a linear combination of colours R, G, and B (Luminance = 0.299 R + 0.587 G + 0.144 B), occasionally colours with similar luminance values may be relatively far from each other. Other drawbacks are the ease of extraction of hidden data, dependency of stego-image quality on number of palette colours, and ease of detection of presence of data using simple statistical histogram analysis[6].

Fridrich[7] proposed a palette modification scheme for hiding data. In this method, both the cost of removing an entry colour in a palette and the benefit of generating a new one to replace it are calculated. If the maximal benefit exceeds the minimal cost, entry colour is replaced. His method remarkably reduces the distortion of the carrier images, but suffers with the low embedding capacity as EzStego does. Cheng[8], *et al.* proposed high embedding capacity technique that can hide

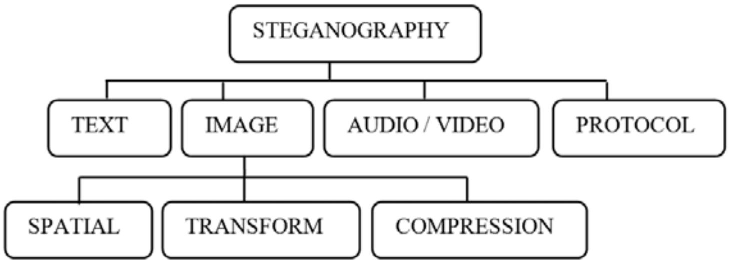

Figure 2. Classifications of steganographic techniques.

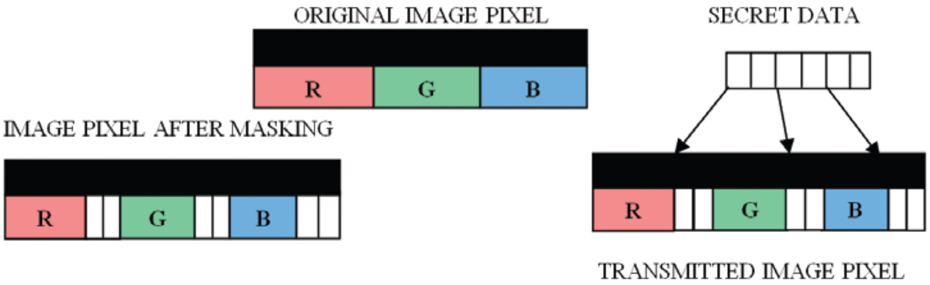

Figure 3. Basic spatial domain data hiding.

1 bit to 8 bits per pixel, and has no distortion in contrast to EzStego. High capacity data hiding algorithm based on relevance of adjacent pixels difference was given by Ren[9], *et al.* Ren's method guarantees the better quality of image after hiding mass information.

2.2 S-Tools, Hide & Seek, StegoDos, White Noise Storm, and other techniques

S-Tools by Andy Brown[5,6] reduces the number of colours from 256 to 32 while maintaining the image quality. Instead of simply going with adjacent colours as EzStego does, S-Tools manipulate the palette to produce colours that have a difference of one bit. As compared to EzStego, non-linear insertions in S-Tools method make the presence and extraction of secret data more difficult and achieve better results in terms of visual perceptibility. Figures 4 and 5 shows cover image before and after embedding data. Hide & Seek given by Maroney[5] uses LSB of each pixel to encode characters of secret data and has embedding capacity which is restricted to 1/8th of the size of the cover-image. StegoDos[5] works only with 320 X 200 pixels image and involves much effort in encoding and decoding of the secret message. White Noise Storm includes encryption to randomise the bits within an image and suffers with the problem of using large cover file.

Younes[10], *et al.* proposed a method in which data is inserted into LSB of each byte within the cover-image in encrypted form. Mandal[11] proposed a method with minimum deviation of image fidelity resulting high quality stego-image with better embedding capacity.

2.3 Bit Plane Complexity Segmentation Steganography

Bit plane complexity segmentation steganography (BPCS) was introduced by Kawaguchi[12], *et al.* It is based on the simple idea that the higher bit planes can also be used for embedding information. In BPCS, each block is decomposed into bit-plane. The LSB plane would be a binary image consisting of the LSB of each pixel in the image and so on. In each segmented bit-plane its complexity is analysed and based on a threshold value block is divided into 'informative region' and 'noise-like region' and the secret data is hidden in noise regions without degrading image quality. BPCS provides high embedding capacity and least degradation of the cover-image as compared to traditional LSB manipulation techniques. Maya[13], *et al.* uses variance of image block as a parameter for complexity measure. Prime advantages achieved are high embedding capacity and robustness against noise as compared to BPCS technique.

2.4 Information Theory-based Data Hiding

Hadhoud[14], *et al.* proposed a technique based on entropy calculation. In this method entropy of the '4' most significant bits (MSBs) are calculated first which contains most detail of each pixel. If the entropy is > 2 then it inserts '4' bits into the '4' LSBs, if not then the entropy of the '5' MSBs is calculated. If it is > 2 then it inserts '3' bits into the '3' LSBs, if not then it inserts '2' bits into '2' LSBs. Flowchart for entropy based data hiding is shown in Fig 6. This method provides high embedding and high level of image transparency.

Figure 4. S-Tools: Before embedding.

Figure 5. S-Tools: After embedding.

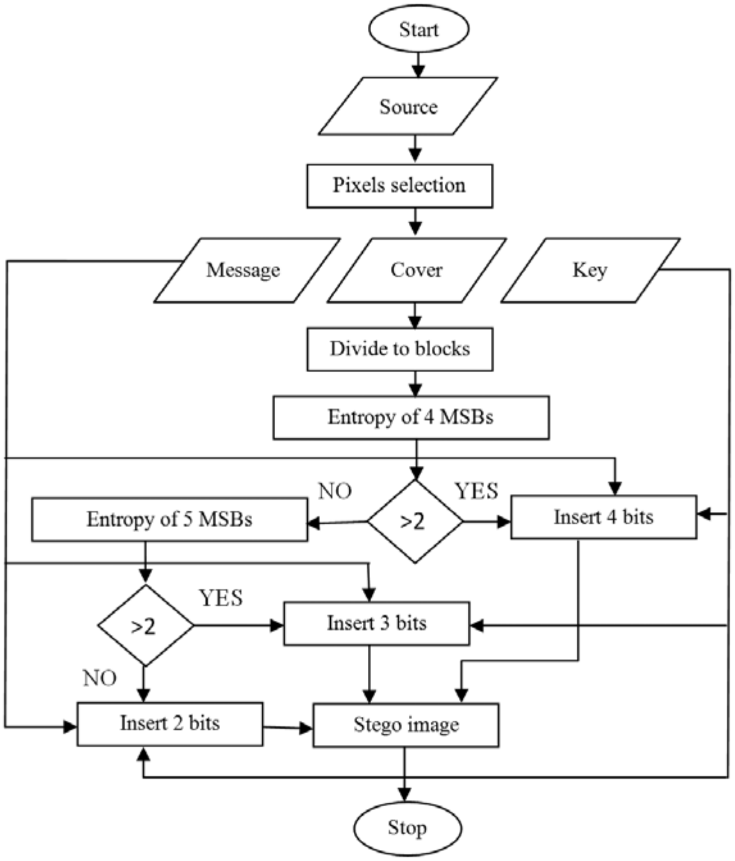

Figure 6. Entropy-based data hiding.

2.5 Dynamic Programming-based Steganographic Technique

Mielikainen[15] proposed LSB matching revisited technique to achieve data hiding. Advantage is that for hiding two secret bits in a pair of cover pixels, only one cover pixel is need to be modified. To illustrate Mielikainen's method, consider two cover pixels (y_1, y_2) and two secret bits (s_1, s_2). Mielikainen's method defines a formula called as binary function as F (y_1, y_2) = LSB ($y_1/2 + y_2$). The function LSB(x) stands for the value of the LSB of the pixel x. More precisely, the more frequently the Case 1 occurs, the better the results Mielikainen's method can obtain. Chan[16], *et al.* transformed secret bits in to their substitutes to increase the occurrence of best cases so as to minimise the number of changes. Chan uses the same concept given by Chang[17], for finding an optimal substitution table. First, this method produces an optimal substitution table by using the chang's dynamic programming strategy. The secret data is then transformed according to the substitution table. Finally, the transformed secret data are embedded into a cover-image using Mielikainen's technique. The number of modified pixels in this method is fewer than that of Mielikainen's method. The only drawback of this method is that substitution table must be delivered to the receiver through a secure channel. Figure 7 illustrates the way Binary Function is used to hide secret data under different cases.

2.6 Data Hiding using Convolution Decoder

Daneshkhah[18], *et al.* proposed convolution decoder-based data hiding method. Results show that embedding capacity can increase up to two bits per pixel for this method. A convolution decoder is used in this method as shown in the Fig 8. Each time 4 LSBs of a pixel enter the decoder machine. Three XOR operations create three outputs n1, n2, and n3. Suppose n2, n3 as the hidden message. If n2, n3 be the same as hidden information, then there is no need to manipulate the original image; if not then change the original image in a way to cause the output of the decoder to be equal to the hidden message.

2.7 High Embedding Data Hiding using Exploiting Modification Direction Method

Exploiting modification direction (EMD) method was proposed by Zhang and Wang[19]. The major highlight of this method is its high embedding capacity. In EMD embedding each secret digit in a (2n+1)-ary notational system is carried by n cover pixels with a price of only one pixel modification. Before the embedding process, the secret information is transformed into a sequence of digits in a notational system with an odd base (2n+1). If the secret information is a binary stream, it need to be segmented into many pieces by L bits, and the decimal value of each piece is represented as K digits in a (2n+1)-ary notational system. The extraction function f is calculated by:

$$f(g_1, g_1, ...g_n) = \left\lfloor \sum_{i=1}^{n} (g_i \times i) \right\rfloor \mathrm{mod}(2n+1)$$

After calculating f value of each group, each secret digit d will be mapped to a group. If $d = f$, the original cover pixels keep unchanged. If $d \neq f$, calculate k as shown below. If $k \leq n$, increase g_k by 1; otherwise, decrease g_{2n+1-k} by 1. K is calculated as: $k = (d-f) \bmod (2n + 1)$. If n is set to 2, only one secret digit is embedded for two consecutive pixels.

Lee[20], *et al.* proposed a high capacity EMD method where one secret digit in 8-ary notational form is embedded in two cover pixels and only one pixel is increased or decreased by one. Compared to EMD, embedding capacity is increased to 1.5 times. Lee[21], *et al.* presented further improvement to EMD. Lee showed that pixel segmentation strategy could hide large payloads. Jung[22] proposed a method in which each secret digit in (2n+1)-ary notational system can be carried by only one cover pixel instead of two as in Lee's method. This method achieves a capacity double that of the EMD method.

2.8 Data Hiding using Information Secret Sharing Method

Threshold secret sharing (k, n) method was proposed by Shamir[23], where a secret d in the form of an integer is to be shared, n is the number of participants in the secret sharing activity, and k is a threshold specifying the minimum number of shares which should be collected to recover the secret d. Lee[24], *et al.* used Shamir's sharing method and proposed information-sharing-based data hiding method. Secret data string is transformed next into shares using the coefficients of some polynomial functions. Coefficient parameters involved in the Shamir's method are used as carriers of the secret data.

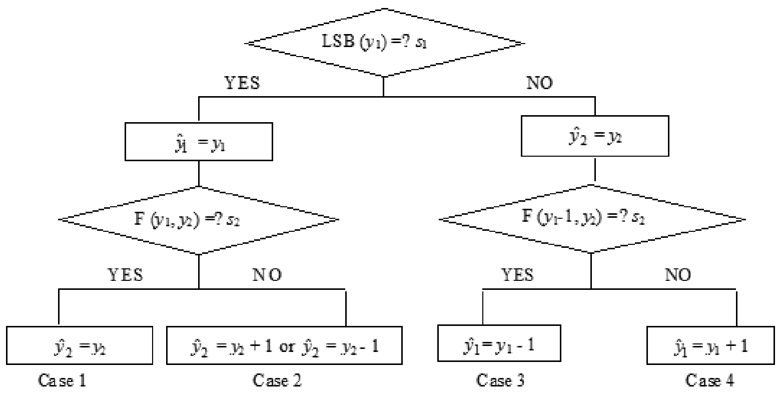

Figure 7. Mielikainen's decision tree.

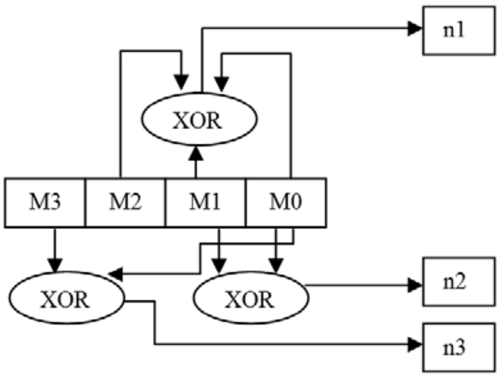

Figure 8. Convolution decoder machine.

3. DATA HIDING TECHNIQUES IN FREQUENCY DOMAIN

Frequency domain methods hide messages in significant areas of the cover-image which makes them more robust to attacks such as compression, cropping or image processing methods than LSB approach and moreover they remain imperceptible to the human sensory system as well. Many transform domain variations exist, one of which is discrete cosine transform (DCT). Some of the important frequency domain-based steganographic data hiding methods are:

3.1 JSteg, JSteg-Shell, JPHide, and OutGuess

JSteg developed by Derek Upham[25,26] sequentially replaces the LSB of the DCT coefficients with the message's data. This technique does not require a shared secret; as a result, anyone who knows the steganographic system can retrieve the message easily, thus not so secure. JSteg-Shell is a windows user interface to JSteg developed by Korejwa[26]. It supports encryption and compression of the content before embedding the data with JSteg. Both methods can be easily detected using χ^2 -test given by A. Westfeld in 1999.

JPHide steganographic system was given by Allan Latham[26]. Two versions 0.3 and 0.5 are available. Version 0.5 supports additional compression of the secret message. As the DCT coefficients are not selected sequentially from the beginning of the image, JPHide is not vulnerable to χ^2 -test; however detected using its extended version[25].

Outguess was proposed by Provos[25, 26] as a response to the statistical tests given by Andreas Westfeld. It improves embedding by selecting DCT coefficients randomly. Two versions are available: Outguess 0.13b which is vulnerable to extended version of χ^2 -test and Outguess 0.2 which has the ability to preserve frequency counts statistics and hence remain undetected. Provos observed that while embedding not all the redundant bits were used and thus it is possible to use the remaining bits to correct statistical deviations that embedding created. Outguess 0.2 uses this phenomenon to avoid class of χ^2 -tests.

3.2 Data Hiding Techniques: F3, F4 and F5

F3 decrements the non-zero coefficient's absolute value only if the LSB does not match with the secret bit. Zero coefficients are skipped completely. Advantage is its resistance to statistical attack (χ^2 -test). Major shortcomings are its less capacity, surplus of even coefficients caused by shrinking and repetitive embedding required since receiver cannot differentiate between skipped 0 and the 0 generated due to shrinkage.

The F5 algorithm was introduced by German researchers Pfitzmann and Westfeld[27]. F5 embeds message bits into randomly-chosen DCT coefficients and employs matrix embedding that minimizes the necessary number of changes to embed a message of certain length. F5 comes after a series of F3 and F4. F5 is similar to F4 except of the fact that F4 does not use matrix encoding in embedding process. The major strengths of F5 are its high embedding capacity without sacrificing security and its resistance to statistical and visual attacks.

3.3 Genetic Algorithm-based Data Hiding

Chang[28], *et al.* proposed a JPEG and quantisation table modification (JQTM) method that improves the standard JPEG quantisation table for better quality of the stego-image. In this method only 26 middle frequency components of the quantised DCT coefficients for each block are used to hide the secret message. JQTM suffers with its low embedding capacity and low security level. Li and Wang[29] modified the quantisation table used in JQTM and uses Particle swarm optimisation [30] to approach optimal LSB substitution, which guarantees a higher security level and better quality for the cover images.

To further increase the embedding capacity of the JQTM, Fazli[31], *et al.* modified quantisation table proposed by Li and Wang. Fazli, *et al.* first transformed secret message using optimal substitution matrix calculated using PSO algorithm and then embed transformed results into the quantised coefficients. This technique differs from Li and Wang's method in the sense that in this substitution matrix is calculated for each 8 x 8 block of the cover-image instead of a single matrix for the whole cover-image. The great achievement of this method is a high security level, high embedding capacity, and high image quality as compared to the JQTM and Li and Wang's method.

4. DATA HIDING TECHNIQUES IN COMPRESSION DOMAIN

In recent years, researchers have concentrated on embedding secret data into the compression domain. Various methods have been proposed for hiding data directly into the compressed codes of the image. Furthermore, the compressed codes transmitted attract less attention of the intruder.

4.1 Data Hiding Using Vector Quantisation & Side-Match Vector Quantisation

In vector quantisation (VQ) [32], a block image is imported; the VQ encoder seeks the most similar codeword from the codebook to substitute for the block and the index value is then exported as the compressed code for the block. Example of VQ encoding is shown in the Fig 9. Side-match VQ (SMVQ), improving VQ compressing performance was proposed by Kim[33]. In SMVQ instead of using the original pixels to encode the X block, Kim uses the upper U block and the left L block to encode the X block. SMVQ encoder is shown in Fig 10. Yang[34], *et al.* presented a reversible data hiding scheme based on SMVQ for VQ compressed images. This method makes the corresponding code words in the current state codebook and the next state codebook close. Results show that Yang's scheme has higher capacity, better visual quality, and lower running time as compared to Chang's method[35].

Chang[36], *et al.* provided a VQ-based embedding method with high embedding capacity. In their method, a codebook is partitioned into clusters. Data are embedded into the VQ index table by transferring index values from one cluster into another cluster. Data hiding schemes for VQ-compressed images are based on index modifications. These schemes may cause distortions and hence are not suitable for authentication of VQ-compressed images. To overcome this limitation Jiafu[37], *et al.* proposed an image authentication scheme for VQ-compressed images. This scheme utilises an information

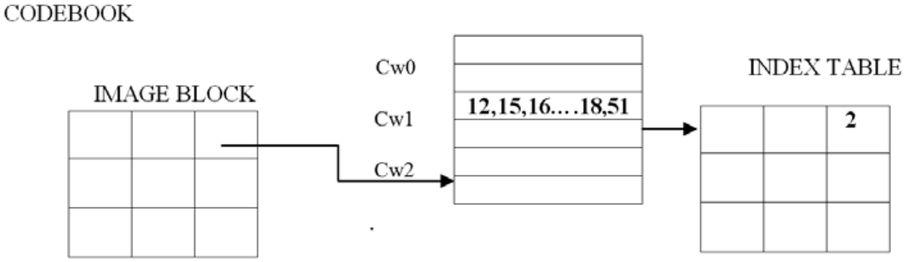

Figure 9. Example of VQ encoder.

						U	
				U12	U13	U14	U15
			L3	X0	X1	X2	X3
	L		L7	X4			
			L11	X8		X	
			L15	X12			

Figure 10. Example of SMVQ encoder.

hiding method based on covering codes[38]. It only modifies few indices slightly to hide authentication information. Yang[39], *et al.* further increases the embedding capacity of VQ-based data hiding scheme. Under the same sorted VQ codebook, the experimental results demonstrate that this data hiding algorithm has higher capacities and better compression rates. For the VQ-based algorithms discussed above only limited amount of information can be hidden, to overcome this, Kekre[40], *et al.* proposed a method based which can achieve hiding capacity of 100 per cent or more, that means secret message can be of same or more size than the cover image.

4.2 Data Hiding in Block Truncation Coding

Xiaotian Wu[41], *et al.* presented a technique of data hiding method by modifying the bitmaps generated from the block truncation coding (BTC) method given by Delp and Mitchell[42]. In the encoding phase of BTC, the original image is firstly divided into non-overlapping blocks with *n* x *n* pixels. For each block, the mean value is calculated. All the pixels in the block are separated into two groups, greater and smaller than or equal to the mean value. A bitmap with the same size of the block is used to record the output of the BTC compression. The bit in bitmap is set to 1 and classified to G1, when the corresponding pixel in the block is greater than the mean value; otherwise, it is set to 0 and classified to G0. Two mean values XH and XL are calculated, representing mean of pixel values in G1 and G0. Using this each block of the original image is compressed into a bitmap and two quantisation levels, XH and XL. Wu uses BTC compression where each bit of the secret message is sequentially embedded into the bitmap of the corresponding compressed non-overlapping block. It results in higher imperceptivity.

4.3 Data Hiding in Compressed Images Using Histogram Analysis

Keissarian[43] proposed a method that decomposes the host image into blocks of variable sizes according to histogram analysis of the block residuals. Variable block sizes are then encoded at different rates based on their visual activity levels. The key point is to embed majority of secrete data into smooth area of the image. Results confirmed that the proposed scheme can embed a large amount of data while maintaining satisfactory image quality. Keissarian[44] proposed further improvement in which the computation of the gray values, are carried out through analysis of the block residuals' histogram.

5. CONCLUSION AND SUMMARY

This paper presented the recent research work in the field of steganography deployed in spatial, transform, and compression domains of digital images. Transform domain techniques make changes in the frequency coefficients instead of manipulating the image pixels directly, thus distortion is kept at minimum level and that's why they are preferred over spatial domain techniques. But when it comes to embedding capacity, spatial domain techniques give better results. However, there exists a trade-off between the image quality and the embedding capacity. Hiding more data results directly into more distortion of the image. So the steganography technique deployed is dependent on the type of application it is designed for. In recent years, some researchers have concentrated on embedding secret data into the compression codes of images. Such need arises keeping in mind the bandwidth requirements.

Steganography can also be used misused like other technologies. For instance terrorists may use this technique for their secret secure communication or anti-virus systems can be fooled if viruses are transmitted in this way. However, it is evident that steganography has numerous useful applications and will remain the point of attraction for researchers.

REFERENCES

1. Nirinjan, U.C. & Anand, D. Watermarking medical images with patient information. *In* the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Hong Kong, China, 1998, pp. 703-06.
2. Katiyar, S.; Meka, K.R.; Barbhuiya, F.A. & Nandi, S. Online voting system powered by biometric security using steganography. *In* the 2nd International Conference on Emerging Applications of Information Technology (EAIT), Kolkata, India, 2011, pp. 288-291.
3. Shirali-Shahreza, M. Improving mobile banking security

using steganography. *In* the 4th International Conference on Information Technology, ITNG, Las Vegas, 2007, pp. 885-887.

4. Machado, R. EzStego, Stego Online. http://www.stego.com (Accessed on 15 April 2011).
5. Johnson, N.F. & Jajodia, S. Exploring steganography: Seeing the unseen. *IEEE Computer*, 1998, **31**(2), 26-34.
6. Westfeld, A.; Pfitzmann A. Attacks on steganographic systems breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-tools—and some lessons learned. *In* the 3rd International workshop on Information hiding, Dresden, Germany, 1999, Springer, pp. 61-76.
7. Fridrich, J. A new steganographic method for palette-based images. IS&T PICS, Savannah, Georgia, 1999, pp. 285-89.
8. Cheng, Z.; Kim, Se-Min &Yoo, Kee-Young. A new steganography scheme based on an index-colour image. *In* the 6th International Conference on Information Technology: New Generations, Las Vegas, Nevada, 2009, pp. 376-81.
9. Ren, Honge; Chang, Chunwu & Zhang, Jian. Reversible image hiding algorithm based on pixels difference. *In* the IEEE International Conference on Automation & Logistics, ICAL '09, Shenyang, 2009, pp. 847-850.
10. Younes, Mohammad Ali Bani & Jantan, A. A new steganography approach for image encryption exchange by using the least significant bit insertion. *Inter. J. Comp. Sci. Network Security*, 2008, **8**(6), 247-254.
11. Mandal, J.K. & Sengupta, M. Steganographic technique based on minimum deviation of fidelity (STMDF). *In* the 2nd International Conference on Emerging Applications of Information Technology (EAIT), Kolkata, 2011, pp. 298-301.
12. Kawaguchi, E. & Eason, R.O. Principle and applications of BPCS-Steganography. *In* the SPIE Conference on Multimedia Systems and Applications, Boston, 1998, **3524**, pp. 464-73.
13. Maya, S.T.; Miyatake, M.N. & Medina, R.V. Robust steganography using bit plane complexity segmentation. *In* the 1st International Conference on Electrical and Electronics Engineering, 2004. Mexico, pp. 40-43.
14. Hadhoud, M.M.; Ismail, N.A.; Shawkey, W. & Mohammed, A.Z. Secure perceptual data hiding technique using information theory. *In* the International Conference on Electrical, Electronic and Computer Engineering (ICEEC), Egypt, 2004, pp. 249-253.
15. Mielkiainen, J. LSB Matching revisited. *IEEE Signal Proc. Letters*, 2006, **13**(5), 285-87.
16. Chan, C.S. & Chang, C.Y. An information hiding scheme by applying the dynamic programming strategy to LSB matching revisited. *In* the 3rd International Conference on Ubiquitous Information Management and Communication (ICUIMC), ACM New York, NY, USA, 2009, pp. 246-250.
17. Chang, C.C.; Hsiao, J.Y. & Chan, C.S. Finding optimal LSB substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, 2003, **36**(7), 1583-595.
18. Daneshkhah, A.; Aghaeinia, H. & Seyedi, S.H. A More secure steganography method in spatial domain. *In* the 2nd International Conference on Intelligent Systems, Modeling and Simulation (ISMS), 2011, pp. 189-94.
19. Zhang, X. & Wang, S. Efficient steganographic embedding by exploiting modification direction. *IEEE Communications Letters*, 2006, **10**(11), 781-83.
20. Lee, C.F.; Wang, Y.R. & Chang, C.C. A steganographic method with high embedding capacity by improving exploiting modification direction. IIHMSP, Kaohsiung, 2007, pp. 497-500.
21. Lee, C.F.; Chang, C.C. & Wang, K.H. An improvement of EMD embedding method for large payloads by pixel segmentation strategy. *Image Vision Computing*, 2008, **26** (12), 1670-676.
22. Jung, K.H; Yoo, K.Y. Improved exploiting modification direction method by modulus operation. *Int. J. Signal Proc., Image Proc. Pattern*, 2009, **2**(1), 79-88.
23. Shamir, A. How to share a secret. *Communication of the ACM*, 1979, **22**, 612-13.
24. Lee, C.W. & Tsai, W.H. A new steganographic method based on information sharing via PNG images. *In* the 2nd International Conference on Computer and Automation Engineering (ICCAE), Singapore, 2010, 807-11.
25. Provos, N. & Honeyman, P. Hide and seek: An introduction to steganography. *IEEE Security Privacy*, 2003, **1**(3), pp. 32-44.
26. Provos, N. & Honeyman, P. Detecting steganographic content on the internet. ISOC NDSS'02, San Diego, CA, 2002.
27. Westfeld, A. F5—A steganographic algorithm: High capacity despite better steganalysis. *In* the Proceedings of 4th International Workshop Information Hiding, Springer-Verlag, 2001, pp. 289-302.
28. Chang, C.C.; Chen, T.S. & Chung, L.Z. A steganographic method based upon JPEG and quantisation table modification. *Information Sciences*, 2002, **141**(1), 123-38.
29. Li, X. & Wang, J. A steganographic method based upon JPEG and particle swarm optimisation algorithm. *Information Sciences*, 2007, **177**(3), 99-109.
30. Elbeltagi, E.; Hegazy, T. & Grierson, D. Comparison among five evolutionary-based optimisation algorithms. *Adv. Engg. Informatics*, 2005, **19**(1), 43-53.
31. Fazli, S. & Kiamini, M. A high performance Steganographic method using JPEG and PSO algorithm. *In* the IEEE International Multitopic Conference, INMIC 2008.
32. Gray, R.M. Vector quantisation. *IEEE ASSP Mag.*, 1984, **1**(2), 4-49.
33. Kim, T. Side match and overlap match vector quantisers for images. *IEEE Trans. Image Proc.*, 1992, **1**(2), 170-85.
34. Yang, C.H.; Huang, C.T. & Wang, S.J. Reversible steganography-based on side match and hit pattern for VQ compressed images. *In* the 5th International Conference on Information Assurance and Security, 2009.
35. Chang, C.C. & Lin, C.Y. Reversible steganography for VQ compressed images using side matching and relocation. *IEEE Tran. Infor. Forensics Security*, 2006, **1**(4), 493-501.

36. Chang, C.C.; Wu, W.C. & Hu, Y.C. Lossless recovery of a VQ index table with embedded secret data. *J. Vis. Comm. Image Representation*, 2007, **18**(3), 207-16.
37. Jiafu, W.; Jiazhen, W.; Yuehui, T. & Aizhen, L. An authentication scheme for VQ-compressed images. *In* the 1st International Workshop on Education Technology and Computer Science, 2009.
38. Galand, F. & Kabatiansky, G. Information hiding by coverings. *In* IEEE Proceedings of Information Theory Workshop, Paris, France, March 2003, pp.151-154.
39. Yang, C. H.; Lin, Y. C.Reversible data hiding of a VQ index table based on referred counts. *J. Vis. Comm. Image Representation,* 2009, **20**(6), 399-407.
40. Kekre, H.B.; Sarode, T.K.; Athawale, A. & Sagvekar, K. High payload using mixed codebooks of vector quantisation. *Int. J. Comp. Sci. Engg.*, 2010, **2**(2), 352-56.
41. Wu, X. & Sun, W. Data hiding in block truncation coding. *In* International Conference on Computational Intelligence and Security, 2010.
42. Delp, E. & Mitchell, O. Image compression using block truncation coding. *IEEE Trans. Comm.*, 1979, **27**(9), 1335-342.
43. Keissarian, F. Using a novel variable block size image compression algorithm for hiding secret data. *In* the IEEE International Conference on Signal Image Technology and Internet Based Systems, Bali, 2008. pp. 285-292.
44. Keissarian, F. Hiding secrete data in compressed images using histogram analysis. *In* the 2nd International Conference on Computer & Automation Engineering (ICCAE), Singapore, 2010, **2**, pp. 492-96.

Contributor

Mr Babloo Saha has received his BE (Computer Engg) from Netaji Subhas Institute of Technology, University of Delhi, in 2008. Currently, he is working as a Scientist in the Institute for Systems, Studies and Analyses, Delhi. His areas of interests include: Modeling and simulation of war-games, multi-agents system and information security.

Ms Shuchi Sharma has received her BE (Computer Engg) from Yagyavalkya Institute of Technology, University of Rajasthan, in 2009. Currently, she is working as a lecturer in Jaipur Institute of Engineering & Technology, Jaipur. Her areas of interests include: Data communication and information security.