ISSN:0975-9646

Compendium of Reversible Data Hiding

S.Bhavani[1] and B.Ravi teja[2]
Gudlavalleru Engineering College

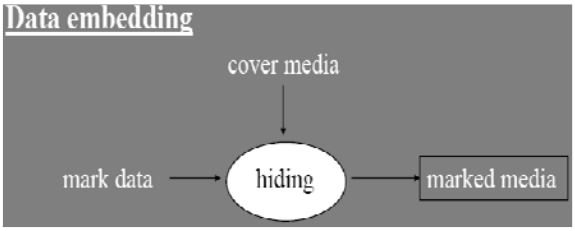
Abstract- In any communication, security is the most important issue in today's world. Lots of data security and data hiding algorithms have been developed in the last decade, which worked as motivation for the research. In the era of internet, in every communication images play a very important role. Images are used for secret communication also like for military purposes, hiding the serial number or copyright also to embed the virus and other bad things etc. To hide data in image in such a way that the existence of the message is unknown is steganography. Different techniques are used to hide data in the image to achieve high quality of stego image and high embedding capacity. In this paper, some of those steganographic techniques are discussed.

Keywords: Reversible data hiding, watermarking, difference expansion, steganography.

I INTRODUCTION

The current trend related to internet. Everyone use internet to collect and share information from one point to another. Internet has become the fastest mean to send and receive the data. In today's era, without internet life seems to be difficult. Images play a vital role in communication on internet. Images are also used for secret communication. The technique of doing secret communication is known as steganography. Steganography is the art and science of invisible communications. This can be done by hiding data in other data. Steganography is derived from the greek word 'Steganos' which means covered or hidden and 'Graphy' means writing. Greeks use different techniques to send the secret message to desired destination. The concepts of invisible ink, punching the message on slaves head, wax table, biliterals are used by Greeks. In steganography the secret data is hidden in covered image. The covered image with secret data is known as Stego-image.

Image Steganography is performed in two steps. To embed the secret message in the covered image and the resultant image is the stego image is the embedding process. Secondly, the extraction of secret message from the stego-image is the extraction process. Figure 1 represents above two steps.



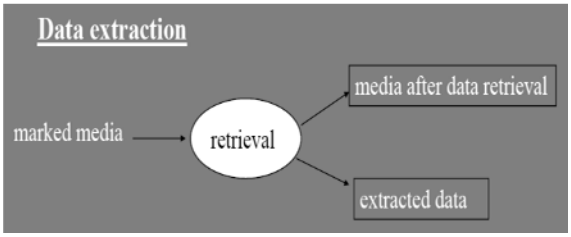


Figure 1: Data embedding and extraction.

The images are of two types. Reversible image is the first type of image in which the quality of the image will remain same as the host image or covered image after extraction. The second type is irreversible image; the quality of image will get under distortion after the extraction of the secret message from the stego-image. The images are also of two formats i.e. raw format and compressed format. The raw format is where the image size is large and compressed format is where the image is compressed and of small size than raw format. As the bandwidth is needed to transmit an image through internet, so the compressed format is used.

Reversible data hiding is such a kind of data hiding techniques in which the original cover media can be recovered without any distortion after hidden data extraction. It is also called as "distortion-free," "invertible," and "lossless." Figure 2 represent the idea of reversible data hiding.

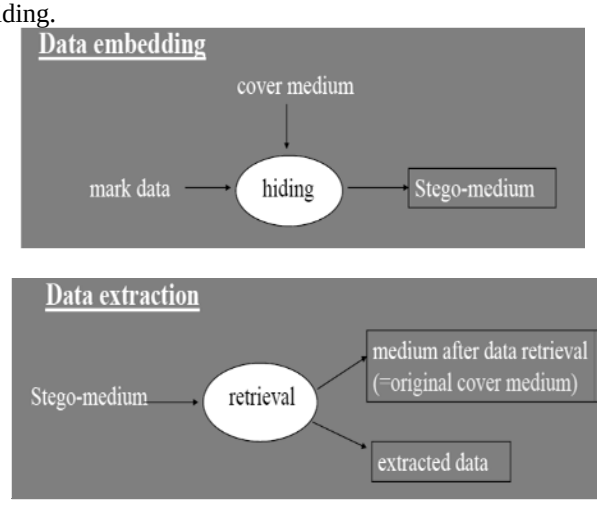


Figure 2: Data embedding and extraction in reversible data hiding.

Reversible data hiding is again in two ways one is Non Separable Reversible Data Hiding and Separable Reversible Data Hiding are shown in figure 3.

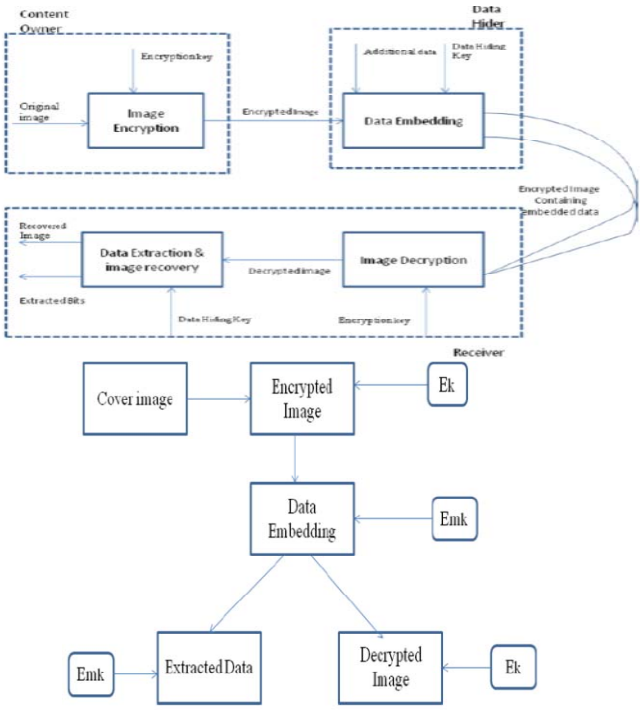


Figure 3: Sketch of Non Separable and Separable Reversible Data Hiding

II RDH TECHNIQUES

II.1. PWLC data hiding technique:

Reversible data hiding technique for binary images is PWLC (Pair-Wise Logical Computation). However, it seems that sometimes PWLC does not correctly extract the hidden data, and fails to recover the original cover image. PWLC does not use spread spectrum and any compression technique, it uses XOR binary operations to store the payload in the host image. It scans the host image in some order. Only sequences "000000" or "111111" that are located near to the image boundaries are chosen to hide data. The sequence "000000" becomes "001000" if bit 0 is inserted, and becomes "001100" if bit 1 is inserted. Similarly, the sequence "111111" becomes "110111" if bit 0 is inserted, and becomes "110011" if bit 1 is inserted. However, the papers [1][2]do not describe clearly how to identify the modified pixels in the extraction process. The image boundaries may change with the watermark insertion. Moreover, let us suppose that a sequence "001000" was found in the stego image. The papers do not give information on how to discriminate between an unmarked "001000" sequence and an originally "000000" sequence that became "001000" with the insertion of the hidden bit 0.

II.2. DHTC data hiding technique:

DHTC (Data Hiding by Template ranking with symmetrical Central pixels) is based on the non-reversible data hiding [3]. DHTC flips only low-visibility pixels to insert the hidden data and consequently images marked by DHTC have excellent visual quality and do not present salt-and-pepper noise.

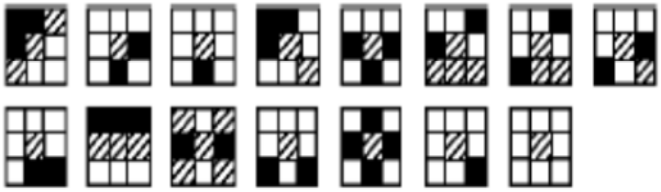


Figure 4: A 3×3 template ranking with symmetrical central pixels in increasing visual impact order.

The process results of DHTC are shown in figure 4. Hatched pixels match either black or white pixels (note that all central pixels are hatched). The score of a given pattern is that of the matching template with the lowest impact. Mirrors, rotations and reverses of each pattern have the same score.

II.3. Lossless Compression and Encryption of Bit-Planes:

Fridrich et al. propose this algorithm in [4]. Space to hide data is found by compressing proper bit-plane that offers minimum redundancy to hold the hash. Lowest bit-plane offering lossless compression can be used unless the image is not noisy. In completely noisy image some bit-planes exhibit strong correlation. These bit-planes can be used to find enough room to store the hash. Hash length is generally 128 bit using MD5 algorithm [5]. The algorithm starts lossless compression from 5th bit-plane and calculates redundancy by subtracting compressed data size from number of pixels. The authors use the JBIG lossless compression method [6] to compress the bit-planes. During embedding the algorithm first calculates the hash of the original image, finds the proper bitplane, and adds the hash with the compressed bit-plane data. Then it replaces selected bit-plane by concatenated data. For more security the concatenated hash with compressed data is encrypted using symmetric key encryption based on 2-dimensional chaotic maps [7].

This algorithm takes variable sized blocks and gives the encrypted message as long as the original message, so no padding is needed. Other public or symmetric key algorithms can be used, but they require padding to embed the encrypted message and hence increase distortion. During decoding after key bit-plane selection the data is decrypted and hash is separated from the compressed original bit-plane data. The bit-plane is replaced by the decompressed data; hence the exact copy of the original image is found. The hash of the reconstructed image is calculated and compared with the extracted hash; if both are same the image in question is authentic [8].

The advantages of this algorithm are – (i) high capacity, (ii) security is equivalent to the security provided by cryptographic authentication, and (iii) can be applied for the authentication purposes of JPEG files, complex multimedia objects, audio files, digitized hologram, etc. The disadvantages are – (i) noisy image forces the algorithm to embed information in higher bit-plane when the distortions are higher and easily visible, (ii) single bit-plane in a small image does not offer enough space to hide hash after compression, so two or more bit-planes are

required and the artifacts must be visible, and (iii) capacity is not high enough to embed large payload.

II.4. Predictive coding:

Predictive coding is used for image and text compression. The differencing value of current data estimation and actual current data encodes the predictive coding. The concept of Median Edge Detector (MED) is used in predictive coding. For each image pixel the predictor values are generated by MED predictor. The predictor values that are generated by MED predictor is called predictive image. Basically, MED predictor is used as a substitute of the difference between the adjacent pixels [9].Error values are obtained as resultant of differencing the original and predictive image. The error values than used in entropy coding stage. Figure 5 represent the template of predictive coding.

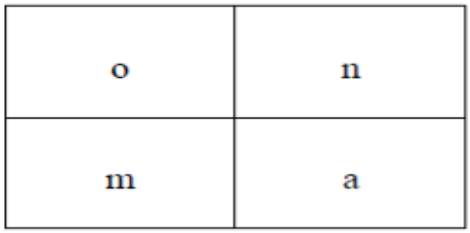


Figure 5: Predictive Template

The neighbouring pixels are used to generate the predictive image in figure 5. Let 'a' be the current predictive pixel having neighbours as m, n, o. In order to detect the vertical and horizontal edges, MED predictor uses the past data i.e. m, n, o in the predictive template. Let the vertical edge on left side of a, the MED predictor use N as the predictive value. When the upper side of 'a' is act as horizontal edge, the MED predictor uses M as the predictive value. If no edge appears in template then MED predictor use M+N-O as the predictive value. In the extracting stage, the error values which are obtained from entropy coding stage are used and predictive image also generate the same MED predictor. The addition of the predictive image and the error values results as the Original image.

Yuan et al. [10] propose a data hiding scheme which is based on prediction that embeds secret data into compression codes during image compression. The scheme is divided into two stages. Predictive stage and an entropy coding stages are the two stages used by Yaun. Yang et al. proposed scheme based on hiding data into edge areas than smooth areas in the host image, which does not differentiate textures from edges and causes serious degradation in actual edge areas. Tsai et al. [11] used the scheme for reversible data hiding is linear prediction for medical images. The scheme is based on histogram shifting which is limited by the hiding capacity. Hossain et al. [12] proposed three different steganographic methods for gray level images. The methods are four neighbours, diagonal neighbours and eight neighbours' methods.

II.5. Least Significant Bit (LSB) substitution method:

Least Significant Bit (LSB) substitution method is a very popular way of embedding secret messages with simplicity. The fundamental idea here is to insert the secret message in the least significant bits of the images. This actually works because the human visual system is not sensitive enough to pick out changes in color where as changes in luminance are much better picked out. A basic algorithm for LSB substitution is to take the first N cover a pixel where N is the total length of the secret message that is to be embedded in bits. After that every pixel's last bit will be replaced by one of the message bits.

Least significant bit (LSB) insertion is a common, simple approach for embedding information in a cover image[13]. The LSB or in other words 8-th bit of some or all the bytes inside an image is changed to a bit of the secret message. Let us consider a cover image contains the following bit patterns:

Byte-1 Byte-2 Byte-3 Byte-4
00101101 00011100 11011100 10100110
Byte-5 Byte-6 Byte-7 Byte-8
11000100 00001100 11010010 10101101

Suppose a number 200 is to embed in the above bit pattern. Now the binary representation of 200 is 11001000. To embed this information at least 8 bytes in cover file is needed. Now modify the LSB of each byte of the cover file by each of the bit of embed text 11001000.

II.6.Difference Expansion Transforms:

Difference expansion, introduced by Tian in 2003, is a reversible transform [14]. According to this algorithm one bit of information is embedded reversibly in each pair of data as shown below. These data can be in spatial or frequency domain, while the capacity of the method approaches 0.5 bpp. An extension of Tian's algorithm is to implement difference expansion on triplets of coefficients [15]. In that way the capacity of the algorithm is increased by 33%, as two bits of information are embedded in each triplet of coefficients. Shen-Hsu's, Alattar's and the proposed transform are all based on triplets and achieve a capacity of up to 0.67 bpp

High Capacity Watermarking Based on Difference Expansion

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added

to the carrier signal, a digital watermark does not change the size of the carrier signal.
The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.
Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority.
In Tian propose a high quality reversible watermarking method with high capacity based on difference expansion. Pixel differences are used to embed data; this is because of high redundancies among the neighbouring pixel values in natural images.
During embedding:
(i) differences of neighbouring pixel values are calculated, (ii) changeable bits in that differences are determined, (iii) some differences are chosen to be expandable by 1-bit, so changeable bits increases, (iii) concatenated bit-stream of compressed original changeable bits, the location of expanded difference numbers , and the hash of original image (payload) is embedded into the changeable bits of difference numbers in a pseudo random order, (iv) use the inverse transform to have the watermarked pixels from resultant differences.

During watermark extraction:
(i) differences of neighbouring pixel values are calculated, (ii) changeable bits in that differences are determined, (iii) extract the changeable bit-stream ordered by the same pseudo random order as embedding, (iv) separate the compressed original changeable bit-stream, the compressed bit-stream of locations of expanded difference numbers (location map), and the hash of original image (payload) from extracted bit-stream, (v)decompress the compressed separated bit-streams and reconstruct the original image replacing the changeable bits, (vi) calculate the hash of reconstructed image and compare with extracted hash.

The advantages are: (i) no loss of data due to compression-decompression, (ii) also applicable to audio and video data, and (iii) encryption of compressed location map and changeable bit-stream of different numbers increase the security.
The disadvantages include: (i) there may be some round off errors (division by 2), though very little, (ii) largely depends on the smoothness of natural image; so cannot be applied to textured image where the capacity will be zero or very low, and (iii) there is significant degradation of visual quality due to bit-replacements of gray scale pixels.

II.7.Reversible Data Hiding by Histogram Shifting:
Ni et al. [16] utilizes zero or minimum point of histogram. If the peak is lower than the zero or minimum point in the histogram, it increases pixel values by one from higher than the peak to lower than the zero or minimum point in the histogram. While embedding, the whole image is searched. Once a peak-pixel value is encountered, if the bit to be embedded is '1' the pixel is added by 1, else it is kept intact. Alternatively, if the peak is higher than the zero or minimum point in the histogram, the algorithm decreases pixel values by one from lower than the peak to higher than the zero or minimum point in the histogram, and to embed bit '1' the encountered peak-pixel value is subtracted by 1. The decoding process is quiet simple and opposite of the embedding process. The algorithm essentially does not follow the general principle of lossless watermarking in.
The advantages of this method are: (i) it is simple, (ii) it always offers a constant PSNR 48.0dB, (iii) distortions are quite invisible, and (iv) capacity is high.
The disadvantages are: (i) capacity is limited by the frequency of peak-pixel value in the histogram, and (ii) it searches the image several times, so the algorithm is time consuming. There are some more efficient algorithms have also been proposed. We refer our survey report of lossless watermarking in [17] to have complete research knowledge of reversible data hiding.

II.8.Reversible Data Hiding With Optimal Value Transfer of Data:
In reversible data hiding techniques, the values of host data are modified according to some particular rules and the original host content can be perfectly restored after extraction of the hidden data on receiver side. In this, the optimal rule of value modification under a payload - distortion criterion is found by using an iterative procedure, and a practical reversible data hiding scheme is proposed. The secret data, as well as the auxiliary information used for content recovery, are carried by the differences between the original pixel-values and the corresponding values estimated from the neighbours. Here, the estimation errors are modified according to the optimal value transfer rule. Also, the host image is divided into a number of pixel subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset. A receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. This way, a god reversible data hiding performance is achieved.

III IMAGE QUALITY PARAMETERS

The degree of distortion of image can be measured by using mean square error (MSE) and peak signal-to-noise ratio (PSNR). Both MSE and PSNR are used because they represent the grey value error of the whole image. All the pixels of an image are equally important. With the use of PSNR or MSE, gray-value difference between corresponding pixels of the original image and the pixels of distorted image are considered. All the pixels of an image are independent of their neighbour pixels. Therefore, pixels at different position have different effect on human visual system (HVS).
Mean Square Error could be estimated in one of numerous approaches to quantify the contrast between values implied by an evaluation and correct quality being certified.

$$MSE = \frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{i=0}^{n-1}[I(i,j)-K(i,j)]^2 \quad \text{-(1)}$$

Where the size of image is mxn

There are numerous measures for examining image quality, such as, the mean structural similarity, mean absolute error, mean square error (MSE), and peak signal-to-noise ratio (PSNR). It is processed by averaging the squared intensity differences of distorted and original image pixels, as well as the related amount of the PSNR.

In the most recent decade, much exertion has gone into the advancement of image quality measures that advantage of well-known characteristics of the human vision framework (HVS). Starting from these truths, the proposed color image quality measure (CQM) takes after another methodology of changing the usage system for the PSNR.

PSNR is expressed in terms of the logarithmic decibel scale because many signals have a very wide dynamic range.

The PSNR is used as a measure of quality of reconstruction of lossy compression .In the case of compression, the signal is the original data, and the noise is the error.

In some cases, reconstruction may appear to be closer to the original than another, even though it has a lower PSNR (a higher PSNR would normally indicate that the reconstruction is of higher quality) [18].

$$PSNR = 10\log_{10}(\frac{MAX^2}{MSE})$$
$$= 20\log_{10}(\frac{MAX}{\sqrt{MSE}})$$
$$= 20\log_{10}(MAX) - 10\log_{10}(MSE)$$

-(2)

Here, MAX is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. Typical values for the PSNR in lossy image and video compression are between 30 and 50 dB, where higher is better. Acceptable values for wireless transmission quality loss are considered to be about 20 dB to 25 dB. When the two images are identical, the MSE will be zero.

IV. CONCLUSION

In this paper, we got into reversible data hiding principles and techniques. Basic notions of RHD and primary techniques including PWLC data hiding technique and DHTC data hiding technique were talked. Afterwards, some of proposed algorithms in the field of RHD were investigated. They were: Lossless Compression and Encryption of Bit-Planes by Fridrich et al., High Capacity Watermarking Based on Difference Expansion by Tian, and Reversible Data Hiding by Histogram Shifting by Ni et al. Features of each algorithm were talked separately in details.

REFERENCES:

[1] C. L. Tsai, K. C. Fan, C. D. Chung and T. C. Chuang,"Data Hiding of Binary Images Using Pair-wise Logical Computation Mechanism," in Proc. IEEE International Conference on Multimedia and Expo, ICME 2004, (Taipei, Taiwan), vol. 2, pp. 951-954, 2004.

[2] C. L. Tsai, K. C. Fan, C. D. Chung and T. C. Chuang, "Reversible and Lossless Data Hiding with Application in Digital Library," International Carnahan Conference on Security Technology, pp. 226-232, 2004.

[3] H. Y. Kim, "A New Public-Key Authentication Watermarking for Binary Document Images Resistant to Parity Attacks," in Proc. IEEE Int.Conf. on Image Processing, (Italy), vol. 2, pp. 1074-1077, 2005.

[4] J. Fridrich, M. Goljan, and D. Rui, "'Invertible Authentication", In Proc. of SPIE Photonics West, Security and Watermarking of Multimedia Contents III, San Jose, California, USA, Vol. 3971, pp. 197-208, January 2001.

[5] R. Rivest, "The MD5 Message-Digest Algorithm", In DDN Network Information Center, http://www.ietf.org/rfc/ rfc1321.txt, April 1992.

[6] K. Sayood, "Introduction to Data Compression", Morgan Kaufmann, 1996, pp. 87-94.

[7] J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps", On Int. Journal of Bifurcation and Chaos, 8(6), pp. 1259-1284, June 1998.

[8] Mohammad Awrangjeb, An Overview of Reversible Data Hiding, ICCIT 2003, 19-21 Dec, Jahangirnagar University, Bangladesh, pp 75-79.

[9] C. L. Tsai, K. C. Fan, C. D. Chung and T. C. Chuang, "Reversible and Lossless Data Hiding with Application in Digital Library," International Carnahan Conference on Security Technology, pp. 226-232, 2004.

[10] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[11] Yu Yuan-Hui, Chang Chin-Chen, Hu Yu-Chen, 2005,"Hiding Secret Data in Images Via Predictive Coding", Journal of Pattern Reorganization, Vol. 38, No. 5, pp 691-705.

[12] Tsai Piyu, Hu Yu-Chen, Yeh Hsiu- Lein, 2009, "Reversible Image Hiding Scheme Using Predictive Coding And Histogram Shifting", Journal of Signal Processing, Vol. 89, No. 6, pp. 1129-1143.

[13] Shamim Ahmed Laskar and Kattamanchi Hemachandran , "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012 .

[14] H.-C. Wu, C.-C. Lee, C.-S. Tsai, Y.-P. Chu & H.-R. Chen, "In a high capacity reversible data hiding scheme with an edge prediction & difference expansion," J. Syst. Softw., vol. 82, pp. 1966-1973, 2009

[15] J. Tian, "Wavelet Based Reversible Watermarking for Authentication", In Proc. Security and Watermarking of Multimedia Contents IV, Electronic Imaging 2002, Vol. 4675, pp. 679-690, 20-25 January 2002.

[16] J. Fridrich, M. Goljan, and D. Rui, "Lossless Data Embedding for all Image Formats", In Proc. SPIE Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, California, USA, Vol. 4675, pp. 572-583, January, 2002.

[17] X. WU, "Lossless Compression of Continuous-Tone Images via Context Selection, Quantization, and Modeling", IEEE Transactions on Image Processing, Vol. 6, No. 5, pp. 656-664, May 1997.

[18] T. Margaret, "Reversible Data Hiding In Encrypted Images by XOR Ciphering Technique", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 2, February 2014