International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 7, Issue 6 (June 2013), PP. 42-49

Review of Various Data Hiding Algorithms in Encrypted Images

Vimal[1], Mahendra Kumar Patil[2]
[1,2]ECE Department, M. M. Engineering College, MMU, Mullana.

Abstract:- Reversible data hiding is a technique to embed additional message into some cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Various skills have been introduced into the typical reversible data hiding approaches to improve the performance. Encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission and decrypt at the receiver end. This paper intends to give thorough understanding and evolution of different existing data hiding algorithm for encrypted images. It covers and integrates recent research work.

Keywords:- DCT, steganography, image encryption , image recovery, reversible data hiding.

I. INTRODUCTION

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. It is argued that the encryption algorithms, which have been originally developed for text data, are not suitable for securing many real-time multimedia applications because of large data sizes. Software implementations of ciphers are usually too slow to process image and video data in commercial systems. Hardware implementations, on the other hand, add more cost to service providers and consumer electronics device manufacturers. A major recent trend is to minimize the computational requirements for secure multimedia distribution by “selective encryption” where only parts of the data are encrypted.

There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all. Selective encryption aims at avoiding the encryption of all bits of a digital image and yet ensuring a secure encryption. The key point is to encrypt only a small part of the bitstream to obtain a fast method. With the rapid progress of Internet, in recent years, to establish the transmission of images, highly reliable and high-speed digital transmission is required. Besides this, Internet applications have to deal with security issues. Internet users exasperate potential security threats such as eavesdropping and illegal access. They want to be protected and to ensure their privacy. Network security and image encryption has become important and high profile issues. Most traditional or modern cryptosystems have been designed to protect textual data. An original important and confidential plaintext is converted into cipher text that is apparently random nonsense. Once the cipher text has been produced, it is saved in storage or transmitted over the network. Upon reception, the cipher text can be transformed back into the original plaintext by using a decryption algorithm. However, images are different from text. Although we may use the traditional cryptosystems (such as RSA and DES-like cryptosystems) to encrypt images directly, it is not a good idea for two reasons. One is that the image size is much greater than that of text, so the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image; a decrypted image containing small distortion is acceptable due to human perception.

There are many applications for digital steganography of images, including copyright protection, feature tagging, and secret communications.

1. Copyright Protection: A secret copyright notice or watermark can be embedded inside an image to identify it as intellectual property . This is the watermarking scenario where the message is the watermark. The “watermark” can be a relatively complicated structure. In addition, when an image is sold or distributed an identification of the recipient and time stamp can be embedded to identify potential pirates.

2. Feature Tagging: Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.
3. Secret Communications: In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use steganography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient.

A. Characterizing Data Hiding Techniques

Steganographic techniques embed a message inside a cover, various features characterize the strengths and weaknesses of the methods. The relative importance of each feature depends on the application

1. Hiding Capacity: Hiding capacity is the size of information that can be hidden relative to the size of the cover. A larger hiding capacity allows the use of a smaller cover for a message of fixed size, and thus decreases the bandwidth required to transmit the stego-image.
2. Perceptual Transparency: The act of hiding the message in the cover necessitates some noise modulation or distortion of the cover image. It is important that the embedding occur without significant degradation or loss of perceptual quality of the cover. In a secret communications application, if an attacker notices some distortion that arouses suspicion of the presence of hidden data in a stegoimage, the steganographic encoding has failed even if the attacker is unable to extract the message.
3. Robustness: Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation, lossy compression, and conversion from digital to analog form and then reconversion back to digital.
4. Tamper Resistance: Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to alter or forge a message once it has been embedded in a stego-image, such as a pirate replacing a copyright mark with one claiming legal ownership. Applications that demand high robustness usually also demand a strong degree of tamper resistance.
5. Other Characteristics: Computational complexity of encoding and decoding is another consideration and individual applications may have additional requirements. For example, for a copyright protection application, a watermark should be resistant to collusion attacks where many pirates works to identify and destroy the mark..

B. Data Embedding

Current methods for the embedding of messages into image covers fall into three categories: Least-Significant Bit embedding (or simple embedding), transform techniques, and methods that employ perceptual masking.

Least-Significant Bit Encoding

A digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bits/pixel are used. In a typical full-color image, there are 24 bits/pixel, 8 bits assigned to each color components. The simplest steganographic techniques embed the bits of the message directly into the least-significant bit plane of the cover image in a deterministic sequence. Modulating the least-significant bit does not result in a human-perceptible difference because the amplitude of the change is small. Other techniques “process” the message with a pseudorandom noise sequence before or during insertion into the cover image.

The advantage of LSB embedding is its simplicity and many techniques use these methods. LSB embedding also allows high perceptual transparency. However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image..

Transform Embedding Techniques:

Another class of techniques is embedding the message by modulating coefficients in a transform domain, such as the Discrete-Cosine Transform (DCT) (used in JPEG compression), Discrete Fourier Transform, or Wavelet Transform. Transform techniques can offer superior robustness against lossy compression because they are designed to resist or exploit the methods of popular lossy compression algorithms. An example of a transform-based steganographic system is the “Jpeg-Jsteg” software, which embeds the message by modulating DCT coefficients of the stego-image based upon bits of the message and the round-off error during quantization.

Perceptual Masking Systems

Recently, a great deal of research has been reported in expanding the hiding capacity and robustness of steganographic techniques by exploiting the properties of the human visual system. The development of accurate human vision models facilitates the design and development of perceptual masking hiding systems. Steganographic techniques designed to be robust to lossy image compression must insert the message into the cover in a manner that is perceptually significant. Techniques that attempt to embed information only in a perceptually insignificant manner, such as LSB embedding techniques, are vulnerable to having the embedded data distorted or quantized by lossy image compression. The masking properties of the human visual system allow perceptually significant embedding to be unnoticed by an observer under normal viewing conditions. “Masking” refers to the phenomenon where a signal can be imperceptible to an observer in the presence of another signal (referred to as the masker.)

II. ANALYSIS OF DIFFERENT METHOD FOR DATA HIDING

A. Reversible Data Hiding in Encrypted Image

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. A number of reversible data hiding methods have been proposed in recent years. In difference expansion method [1], differences between two adjacent pixels are doubled to generate a new least significant bit (LSB) plane for accommodating additional data. A data hider can also perform reversible data hiding using a histogram shift mechanism, which utilizes the zero and peak points of the histogram of an image and slightly modifies the pixel gray values to embed data into the image [2]. Another kind of method makes use of redundancy in a cover by performing lossless compression to create a spare space for data embedding [3]. Furthermore, various skills have been introduced into the typical reversible data hiding approaches to improve the performance [4]–[6].

A sketch of the proposed scheme is given in Fig. 1. A content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image, and then a data hider embeds additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version. The detailed procedures are as follows.

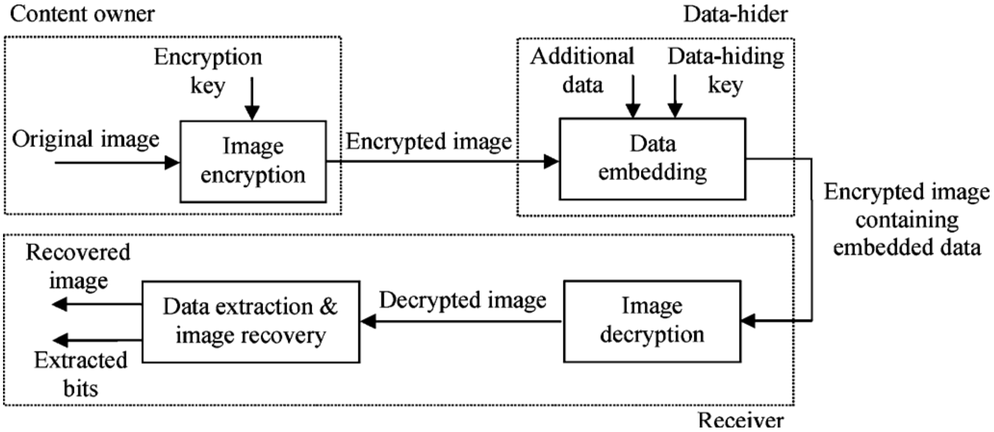


Fig.1: Block diagram of general procedure for reversible data hiding in encrypted images.

The test image Lena sized 512* 512 shown in Fig. 2(a) was used as the original cover in the experiment. After image encryption, the 8 encrypted bits of each pixel are converted into a gray value to generate an encrypted image shown in Fig. 2(b). Then, we embedded 256 bits into the encrypted image by using the side length of each block s=32 . The decrypted image is given as Fig. 2(c), and the values of PSNR caused by data embedding is 37.9 dB, which is imperceptible and verifies the theoretical analysis in [7].

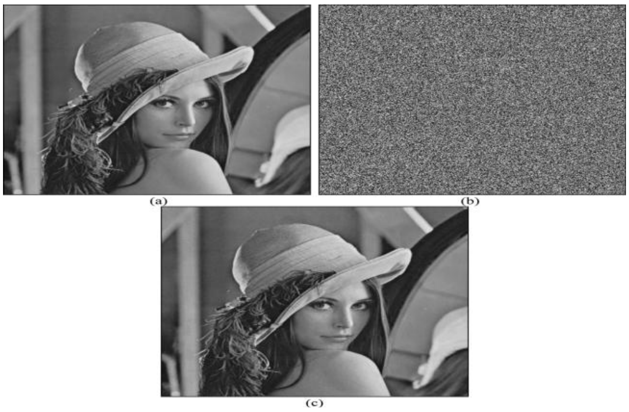


Fig.2: (a) Original Lena, (b) its encrypted version, and (c) a decrypted version containing embedded data.

After image encryption, the 8 encrypted bits of each pixel are converted into a gray value to generate an encrypted image shown in Fig. 2(b). Then, we embedded 256 bits into the encrypted image by using the side length of each block s=32 . The decrypted image is given as Fig. 2(c), and the values of PSNR caused by data embedding is 37.9 dB, which is imperceptible and verifies the theoretical analysis in [7]. At last, the embedded data were successfully extracted and the original image was perfectly recovered from the decrypted image. In the proposed scheme, the smaller the block size, the more additional data can be embedded. However, the risk of defeat of bit extraction and image recovery rises. Fig. 3 shows the extracted- bit error rate with respect to block sizes when four test images Lena, Man, Lake and Baboon sized 512* 512 were used as the original covers.

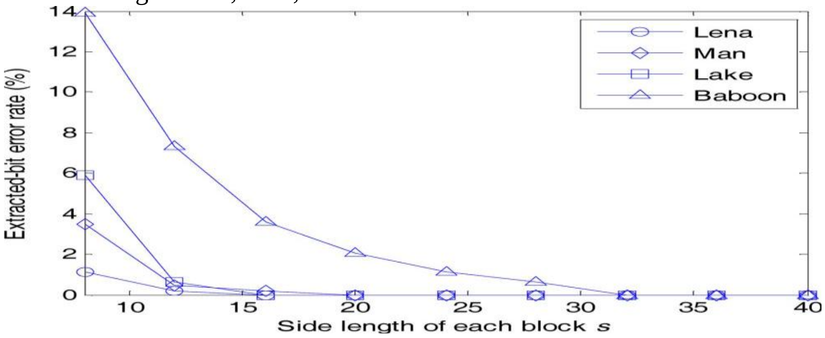


Fig. 3: Extracted-bit error rate with respect to block sizes

Here, the extracted- bit error rate is equivalent to the rate of unsuccessful block recovery. It can be seen that the smoother the cover image, the better is the performance of data extraction and image recovery. When the side length of block is not less than 32, for most cover images, all the embedded bits can be correctly extracted and the original image can be successfully recovered.

B. A Novel Scheme on Reality Preserving Image Encryption

Image security has been attracting more and more attention in recent years with the development of Internet. Image compression, image enhancement and image encryption have been widely studied for applications in engineering industrial, medical processes and optical system etc [8-11]. Image encryption is a direct way for digital image being immune from attack of the traditional cryptograph. Conventional methods of image encryption are usually based on the traditional Fourier transform (FT) or the wavelet technique. With the development of the fractional Fourier transform (FRFT) [16-17], image encryption techniques in the fractional Fourier domain have been proposed in various ways [11]. The FRFT based image encryption methods have been proved to make distinct advantages due to the additional parameters of the rotation angle of the FRFT. At the same time, fast algorithm of the FRFT leads to no additional cost in digital computation.

The proposed reality preserving encryption technique is based on the HT and the double random phase encoding. We apply a pixel scrambling matrix *J* first for the real image $x(t_1,t_2)$ to diffuse the information over the image resulting in the real output $J(x(t_1,t_2))$, thereafter we perform the half planed HT to $J(x(t_1,t_2))$ followed by the double random phase encoding. Different from the double random phase encoding described in which utilize twice FRFT, we apply the FRFT only once. After the process above, we obtain the complex-valued data which can be seen as the half spectrum of another real image, i.e. the real encrypted image.

The encryption procedure at the output plane can be given as:

$$Y=H^{-1}\{[F_{\alpha,B}[H[J(x)M_1]]M_2\} \quad (1)$$

where $M_1 = \exp(j\Pi C_1)$ and $M_2 = \exp(j\Pi C_2)$ present two random phase masks respectively. C_1 and C_2 are two statistically independent white sequences uniformly distributed in the interval [0, 2]. The data after being taken the half-planed HT are multiplied by two statistically independent random phase functions. One is in the Fourier plane and the other is in the encryption plane. In the output plane, we obtain the real encrypted data, which constitute a stationary white noise. It can be seen that the encryption keys consist of the pixel scrambling matrix J, the two phase functions, i.e. C_1 and C_2 , and the angles α and β of the FRFT. The encryption process is shown in Fig. 4.

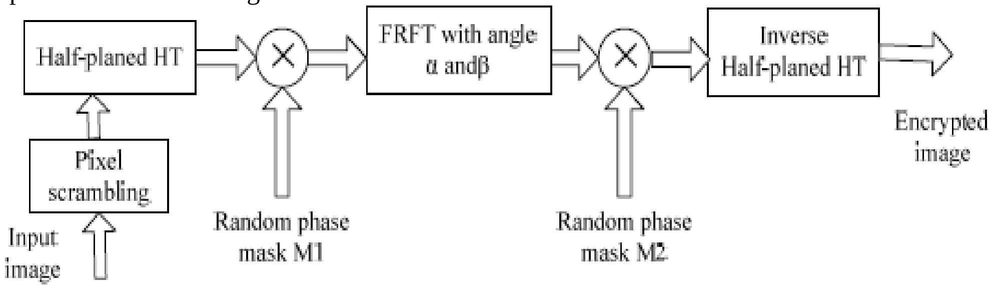


Fig. 4: Scheme of encryption

Since the time domain and the Fourier domain are two special cases when the angle of the FRFT are zero and Π / 2 , we can say that the proposed encryption is implemented in different fractional Fourier plane, which renders the proposed scheme flexible and secure. At the same time, the proposed technique is reality preserving without data expand, which is important in transmitting and processing data. The structure illustrated in figure 1 is symmetric except for the pixel scrambling. Therefore the decryption can be implemented via the same process as the encryption and can be expressed as

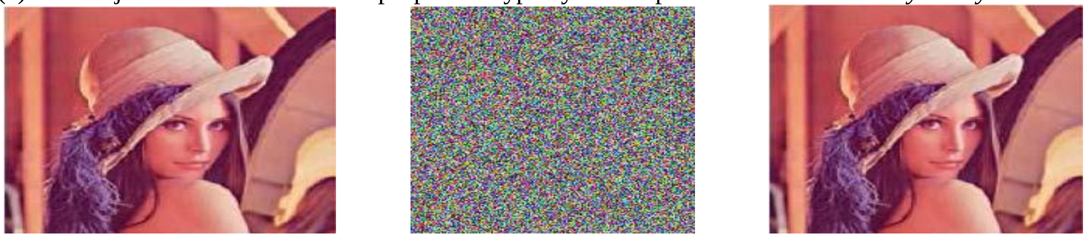
$$x = J^{-1}\{ H^{-1}\{[F_{-\alpha,-\beta} [H (y) M_1^{*}]] M_2^{*}\}\} \qquad (2)$$

where * means the conjugation operator. It is obvious that the decryption keys are $-\alpha,-\beta,-C_{1,-}C_{2,}J^{-1}$

C. Color Image Cryptosystem using Chaotic Maps

The fascinating developments in digital image processing and network communications during the past decade have created a great demand for real-time secure image transmission over the Internet and through wireless networks. To meet this challenge, a variety of encryption schemes have been proposed [21]. Among them, chaos-based algorithms have shown some exceptionally good properties in many concerned aspects regarding security, complexity, speed, computing power, computational overhead, etc. [22]. Due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels, traditional encryption algorithms such as DES, IDEA and RSA are not suitable for practical image encryption, especially under the scenario of on-line communications. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption.

As an example for the subjective evaluation of the proposed cryptosystem, Fig.5 shows the encryption and the decryption of a 256*256 color image of Lena. The plain image of Lena that is shown in Fig. 5(a) is encrypted with a secret key and is presented in Fig. 5(b). Then the cipher-image is decrypted with exactly the same key in Fig.5(c). The objective evaluation of the proposed cryptosystem is presented in the *Security Analysis* section.



(a) **(b)** **(c)**

Fig. 5: (a) Original image of Lena. (b) Encrypted image of Lena. (c) Decrypted image of Lena.

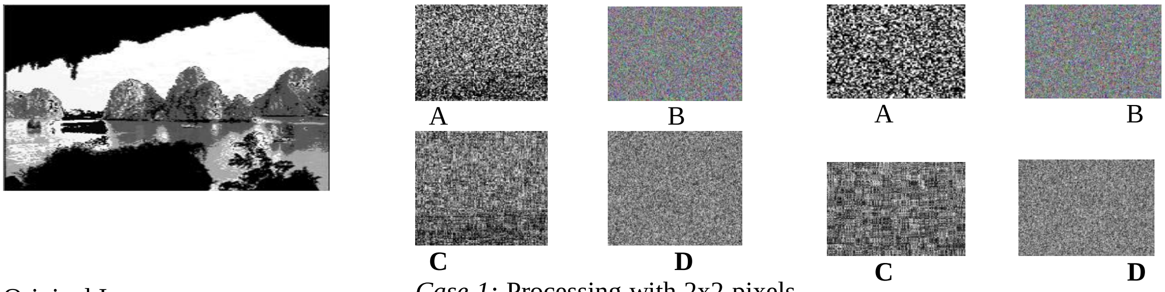
D. Image Cryptography: The Genetic Algorithm Approach

The importance of multimedia technology in our society has promoted digital images to play a still more significant role, and demands a serious protection of users' privacy. To fulfil such security and privacy in various applications, encryption of images is very important to frustrate malicious attacks from unauthorized group. In this regard, a solution is to use an encryption algorithm to mask the image data. For a long period, cryptography has been turned into a battleground of some of the world's most illustrious mathematicians and computer scientists, starting from Shannon's ideas dates back from 1949, which has led to the celebrated number-theory-based encryption algorithms such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and RSA [23,24]. Statistical analysis on large numbers of images shows that medially adjacent 8 to 16 pixels are correlative in horizontal, vertical, and diagonal directions. Correlation among adjacent pixels is evaluated in terms of correlation coefficient, which is a statistical measurement of an image state. The algorithms were applied on a gray scale (8-bit) bit mapped (bmp) image of size 240 × 240 pixels with 256 gay values. In order to evaluate the impact of the number of blocks on the correlation, four different cases have been tested. The number of blocks and the block sizes for each case are shown in Table I.

Table I: Block Sizes for different test cases

	Block size	**Total no. of blocks**
Case 1	2*2 pixels	120*120
Case 2	3*3 pixels	80*80

The initial processing using the pre-encryption technique on the original image (A) generates a transformed image (B). Each case then produces three other output images; image (C) using the Blowfish algorithm, image (D) using the proposed algorithm (GA), and image (E) using Blowfish algorithm followed by the proposed algorithm (BlowGA). The implementation of the work has been done on Intel Pentium IV platform. Operating system used are Microsoft Windows XP and Redhat Enterprise Linux 5. Blowfish algorithm has been executed with readily available code using gcc compiler under Linux. Turbo C++ compiler and Matlab 7.5 have been used under Windows platform. Statistical test includes the comparative performance analysis on the basis of correlation coefficient. A coefficient of correlation is a mathematical measure of how much one number can be expected to be influenced by changes in another. Correlation coefficient of 1 means that the two numbers are perfectly correlated, whereas -1 means that the numbers are inversely correlated and 0 means that the numbers are not related. Next we analyse the effects of the described methods on the original image decomposed into different block size.



Original Image

Case 1: Processing with 2x2 pixels blocks

Case 2: Processing with 3x3 pixels blocks

Fig. 6: (A) Image after initial processing with n x n block, (B) Image after applying Blowfish on B, (C) Image after applying GA on B, (D) Image after applying Blow GA on B.

Table II : Correlation coefficient value of the Original image

Image	**horizontal**	**vertical**	**average**
Image original(A)	0.8417	0.9356	0.88865

Table III : Results of correlation values of Case 1

Image	**horizontal**	**Vertical**	**average**
Initial processing of A (B)	0.4670	0.4843	0.47565
Applying Blowfish on B	0.0252	0.0482	0.0367
Applying GA on B	0.0399	0.0417	0.0408
Applying BlowGA on B	0.0254	0.0249	0.02515

Table IV: Results Of Correlation values of Case 2

Image	horizontal	Vertical	average
Initial processing of A (B)	0.6336	0.6278	0.6307
Applying Blowfish on B	0.0260	0.0680	0.047
Applying GA on B	0.0439	0.0467	0.0453
Applying BlowGA on B	0.0265	0.0281	0.0273

III. DISCUSSION AND ANALYSIS

Nowadays the protection of image data from unauthorized access is important. Image encryption plays a significant role in field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. Reversible data hiding in encrypted image is most commonly method used a days for better security of data. To maintain the quality of image and to reduce the noise we use Discrete cosine transform.

Data hiding is one of the major field which improves several parameters day by day, researchers continually exploring new algorithms to enhance the quality of image even after hiding a major amount of data in it, here is to hide data in images using reversible data hiding algorithm with the use of DCT to match the closest data hiding pixel for every symbol to be hide. There are two methods: Closest element approach and random sequence approach. With the help of these two approaches the closest data hiding is to be match. Basically the purpose of this method is to find out the noisy pixels and then hide the data in it and recover it by decryption process and calculate the error rate to compare the decrypted data with original one.

IV. CONCLUSION

In this paper a comparative study for various data algorithm have been done. Image encryption is a direct way for digital image being immune from attack of the traditional cryptograph. Encryption of images is very important to frustrate malicious attacks from unauthorized group. Chaos-based algorithms have shown some exceptionally good properties in many concerned aspects regarding security, complexity, speed, computing power, computational overhead, etc.. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption.

REFERENCES

[1]. J. Tian, “Reversible data embedding using a difference expansion,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[2]. Z. Ni,Y.-Q. Shi,N. Ansari, andW. Su, “Reversible data hiding,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, 2006.

[3]. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized-LSB data embedding,” *IEEE Trans. Image Process.*, vol. 14,no. 2, pp. 253–266, Feb. 2005.

[4]. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, “Reversible imagewatermarking using interpolation technique,” *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 1, pp. 187–193, 2010.

[5]. W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, “A high capacity reversible data hiding scheme using orthogonal projection and prediction errormodification,” *Signal Process.*, vol. 90, pp. 2911–2922, 2010.

[6]. C.-C. Chang, C.-C. Lin, and Y.-H. Chen, “Reversible data-embedding scheme using differences between original and predicted pixel values,” *Inform. Secur.*, vol. 2, no. 2, pp. 35–46, 2008.

[7]. D.Kundur andK.Karthik, “Video fingerprinting and encryption principles for digital rights management,” *Proc. IEEE*, vol. 92, pp. 918–932, 2004.

[8]. S. Grgic, B. Ozmen, Performance analysis of image compression using wavelets, IEEE Trans. Industrial Electronics, 2001, 48: 682-695

[9]. T. Li, S. I. Kamata, An iterative image enhancement algorithm and a new evaluation framework, IEEE International Symposium on Industrial Electronics, 2008 : 992-997.

[10]. D.R. Bull, D.W. Redmil, “Optimization of image coding algorithms and architectures using genetic algorithms,” IEEE Trans. On Industrial Electronics, 1996 .43: 549-558.

[11]. J. Zhao, H. Lu, X.S. Song, J.F. Li, and Y.H. Ma, Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique, Opt. Commun., 2005, 249: 493-499.

[12]. P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Opt Lett., 1995, 20: 767-769.

[13]. G. Unnikrishnan, J. Joseph, and K. Singh, Optical encryption by double random phase encoding in the fractional Fourier domain, Opt. Lett. , 2000, 25: 887-889.

[14]. N.Singh, A.Sinha, Optical image encryption using Hartley transform and logistic map, Opt. Commun., 2009, 282: 1104-1109.

[15]. L. B. Almeida, The fractional Fourier transform and time-Frequency representations, IEEE Trans. Signal Processing, 1994, 42: 3084-3091.

[16]. R. Tao, L. Qi, and Y. Wang, Theory and applications of the fractional Fourier transform, THU Press, Beijing, 2004.

[17]. Ozturk S, Soukp_nar B. "Analysis and comparison of image encryption algorithms". Int J Inf Technol 2004;1(2):64–7.

[18]. S. Li, Analyses and new designs of digital chaotic ciphers, Ph.D. thesis, School of Electronic and Information Engineering, Xian Jiaotong University, Xian, China; 2003.

[19]. Li S, Chen G, Zheng X. Chaos-based encryption for digital images and videos. In: Multimedia security handbook. LLC, Boca Raton, FL, USA: CRC Press; 2004. p. 133–67

[20]. Mao Y, Chen G. Chaos-based image encryption. In: Bayro-Corrochano E, editor. Handbook of computational geometry for pattern recognition, computer vision, neural computing and robotics. Springer; 2003.

[21]. Kocarev L. Chaos-based cryptography: a brief overview. IEEE Circuit System 2001;1(3): 6–21.

[22]. Khan UM, Kh M. Classical and chaotic encryption techniques for the security of satellite images. In: IEEE international symposium on biometrics and security technologies (ISBAST 2008), vol. 5, no. 23–24;2008. p. 1–6. [1] Shannon CE [1949] "Communication theory of secrecy system,"Bell System Technical Journal, Volume 28, pp. 656 – 715.

[23]. Menezes AJ, van Oorschot PC and Vanstone SA, Handbook of Applied Cryptography; CRC Press, Boca Raton, FL, 1996.

[24]. Stallings W, "Cryptography and Network Security: Principles and Practice". Prentice-Hall, Upper Saddle River, NJ, 1999.