ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue I, March 2015

SECURE TRANSMISSION USING REVERSIBLE DATA HIDING TECHNIQUE

E.Famidha[1], R.Gayathri[2]
PG Scholar[1], Assistant Proferssor[2]
Department of Electronics and Communication,
Mailam Engineering College, Mailam
Villupuram, Tamil Nadu, India.

***Abstract*- The project proposes an enhanced security system for secret data communication. Reversible data hiding technique is used for the data embedding process. A given input image is used for the embedding of the data by using the LSB embedding. In this data embedding the data is embedding using a key. The resultant image is known as the cover image. This data embedded image is then hided into the watermarked image by using DWT using a relevant key. This image is then encrypted by using selective encryption. At the receiver side the image can be recovered separately if the receiver has the watermarking key. If the receiver has only the data embedding key then the data can be extracted separately. The performance of the proposed system is evaluated using PSNR and MSE values. The simulation results show that the proposed system provides high level of security.**

***Index Terms*–Reversible Data Hiding,Adaptive LSB Embedding,data extraction,image recovery,secret bits.**

I.INTRODUCTION

A novel reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the hidden data have been extracted.The secret message bits are encoded with ECC and embedded into the encrypted bitstream by modifying the appended bits corresponding to the AC coefficients. By using the encryption and embedding keys, the receiver can extract the embedded data and perfectly restore the original image[1].By reserving some space in the encrypted images presented in [2],it is easy for the data hider to reversibly embed data in the encrypted image. This method can achieve real reversibility, separate data extraction and image recover.The reversible data hiding in encrypted images is proposed in [3].The method of non seperable reversible data hiding is proposed in [4].The content owner encrypts the original compressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key.In this the data extraction is not seperable from the image decryption.The method of

reversible data hiding is proposed in [5].The algorithm has been successfully applied to a wide range of images.In most cases ofdata hiding, the cover media will experience some distortiondue to data hiding and cannot be inverted back to the originalmedia. That is, some permanent distortion has occurred to thecover media even after the hidden data have been extracted out. In some applications, such as medical diagnosis and law enforcement,it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications, such as remote sensing and high-energy particle physical experimental investigation,it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying this requirement are referred to as *reversible*, *lossless*, *distortion-free*, or *invertible* data hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out, thus

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue I, March 2015

providing an additional avenue of handling two different sets of data.Most of the reversible data hiding techniques focuses on the dataembedding/extracting on the plain spatial domain [6]–[10].Digital Image Watermarking is a technique which provide solution for Copyright, image authentication and otherissuesWatermarking deals with decomposing original image using some wavelet Transforms and embedding watermark into one of the sub band (LL,LH,HL,HH) the obtained image is called watermarked image this image have transmitted throught Channel Where various noise Affect watermarked Image [11],[12],[13].

II.PROPOSED SCHEME

This project proposes a novel method by embedding the data into an image,then the watermarking operation is performed.The proposed sheme is shown in fig.1.The original image is used to embed a data into the image.this embedding is done by choosing an embedding key.Watermarking process is done to the data embedded image by using a different key.Using an encryption key the watermarked image is encrypted.At the receiver side,the image is decrypted by using the same encryption key.If the receiver has only the data embedding key he can still extract the data.

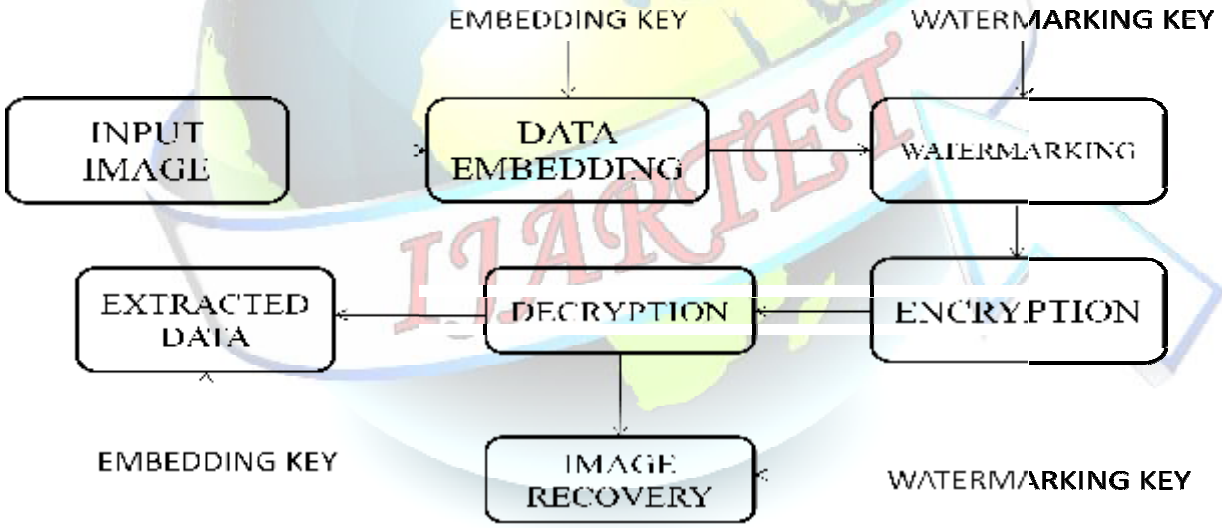

Fig:1 Sketch of the proposed scheme

A.Data Hiding

Maintaining the secrecy of digital information when being communicated over the Internet is presently a challenge. Given the amount of cheap computation power available and certain known limitations of the encryption methods it is not too difficult to launch attacks on cipher-text. An ideal steganographic technique embeds message

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue I, March 2015

information into a carrier image with virtually imperceptible modification of the image.This paper introduces a new, principled approach to detecting least significant bit (LSB) steganography in digital signals such as images and audio. It is shown that the length of hidden messages embedded in the least significant bits of signal samples can be estimated with relatively high precision. The new steganalytic approach is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. The resulting detection algorithm is simple and fast. To evaluate the robustness of the proposed steganalytic approach, bounds on estimation errors are developed.Adaptive steganography comes closer to this ideal since it exploits the natural variations in the pixel intensities of a cover image to hide the secret message. The objective of steganography is a method of embedding an additional information into the digital contents, that is undetectable to listeners..The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels.As the application domain of embedding data in digital multimedia sources becomes broaden, several terms are used by various groups of researchers, including steganography, digital watermarking, and data hiding.In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The lsb is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digits further to the right.The least significant bit (LSB) insertion method is a simple steganographic algorithm that takes the least significant bit in some bytes of the cover medium and swaps them with a sequence of bytes containing the secret data in order to conceal the information in the cover medium. However its imperceptibility and hiding capacity are relatively low. This is as revealed by the statistical characteristics of its resultant stego images compared to the original cover images.To increase the level of imperceptibility and the hiding capacity in the LSB insertion method, this research proposes an enhanced LSB method that employs a selective and randomized approach in picking specific number of target image bits to swap with the secret data bits during the embedding process. To facilitate the selective picking of the target image bits, the standard minimal linear congruential number generator (LCG) is used.

(a) (b)

Fig 2 (a) Input Image (b) Data Embedded image

B. Watermarking

The stego image is then embedded into the watermarked image. A separate key is being used for the watermarking process which is given to the receiver for properly restoring the image. The main idea is that information about the secret key leaks from the observations, for instance, watermarked pieces of content, available to the opponent. The security level is then defined as the number of observations the attacker needs to successfully estimate the secret key. On the contrary, *security* has received little attention in the watermarking community. The first two concepts hardly perceived as different. The intentionality behind the attack is not enough to make a clear cut between. An image compression is clearly an attack related to robustness, but it might happen intentionally, i.e., with the purpose of removing the watermark, or not. The discrete wavelet transform (DWT) algorithms have a firm position in processing of signals in several areas of research and industry. As DWT provides both octave-scale frequency and spatial timing of the analyzed signal, it is constantly used to solve and treat more and more advanced problems.

C. Encryption

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue I, March 2015

A given input image is encrypted using cryptographic technique based on selective encryption method. After image encryption, the data hider will conceal the secret data into the encrypted pixels. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the encrypted image.The encryption process requires an encryption algorithm and a key. The process of recovering plaintext from cipher text is called decryption. The accepted view among professional cryptographers is that the encryption algorithm should be published, whereas the key must be kept secret.A very effective method to encrypt an image, which applies to a binary image, consists in mixing image data and a message (the key in some sense) that has the same size as the image: a XOR function is sufficient when the message is only used once. A generalization to gray level images is straightforward: encrypt each bit plane separately and reconstruct a gray level image.

D. Data Extraction and Image Recovery

The secret data can be extracted from the embedded image with help of key matrix. The hidden encrypted pixels are determined for data extraction by using data hiding key and data will be recovered from the image. This extraction process is opposite to data embedding, pixel intensities and embedding rate are used here to extraction of data. The image also decrypted using selective method with help of key which is used in the encryption module. This paper proposes a low complexity for key generation. The image that is being recovered will be same at that of the original image.The receiver who wants information only about the data that is being embedded can get that information alone of he has only the data hiding key.It is not necessary that he should have information about the encryption key.

III.Quality measures for image

The Quality of the reconstructed image is measured interms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σ_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\text{MSE}=\frac{1}{N}\sum_{j,k}\left(f[j,k]-g[j,k]\right)^2$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (db) is given by:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human eyes.

IV.Experimental Results

All the images used in the experiments are standard gray scale images.The cover image given as an input is resized and data is embedded into the cover image.The stego image isthen hided using a watermarked image.The watermarked image is then encrypted by using an encrypted key.Fig 3 shows the process of the proposed scheme.

Tables I and II lists the comparison of PSNR and MSE values of the proposed scheme and the method in [3].The PSNR values in the proposed scheme is 61.223db which is greater then the method in [3] and the recovered image will have very less degradation.The MSE values of the proposed scheme is less when compared to method in [3].

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue I, March 2015

Table III shows the PSNR values for different input images.These values will vary according to the input image that is used.

(a) (b)

(c) (d)

Fig:3 (a)Data Embedded Image (b)Watermarked Image (c)Encrypted Image (d) Extracted Image

TABLE I
Comparison of PSNR values in the proposed scheme and the method in [3].

	PSNR values
Proposed scheme	61.223
Existing method	50.0346

TABLE II
Comparison of MSE values in the proposed scheme and the method in [3]

	MSE values
Proposed scheme	0.1217
Existing method	0.64509

TABLE III
PSNR values for different input images

Images	PSNR values
Dog	61.2239
Lena	55.4078
Ship	53.3240
Baby	58.7358

V.CONCLUSION

This project proposes a scheme of data hiding in a JPEG bitstream.The data embedded image is then hided into a watermarked image.By doing so the image as well as the data that is embedded will be safe. Then at the receiver side the user can either

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue I, March 2015

extract the data that has been hidden by using the data hiding key or the original image can be obtained by using the decryption key.It does not replace cryptography but rather boosts the security using its obscurity features. The data hiding technique uses the LSB replacement algorithm for concealing the secretmessage bits into the encrypted image. By using the decryption key, the image will be extracted from encryption to get the information about the images.Then the performance parameters such as MSE and PSNR for the image is calculated.This project is used for compressed images.In the future this can also be used for uncompressed images.

REFERENCES

[1] Zhenxing Qian, Xinpeng Zhang, and Shuozhong Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream", IEEE Transactions On Multimedia, Vol. 16, No. 5, August 2014.

[2] K. Ma, W. Zhang, and X. Zhao et al., "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf.Forensics Security, vol. 8, no. 3, pp. 553–562, March 2013.

[3] Xinpeng Zhang, "Seperable Reversible Data Hiding in Encrypted images", IEEE *Trans. Information Forensics And Security*, Vol. 7, no. 2, April 2012.

[4] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[5] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006.

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

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

[8] W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification," Signal Process., vol. 90, pp. 2911–2922,March 2010.

[9] 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.

[10] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[11] Chu, W, 2003. "DCT-Based Image Watermarking Using Subsampling," IEEE Trans. Multimedia, vol. 13, no. 8, pp. 890–896,Aug. 2001.

[12]Deng, F. and B. Wang, 2003. "A novel technique for robust image watermarking in the DCT domain," in Proc. of the IEEE 2003 Int. Conf. on Neural Networks and Signal Processing, vol. 2, pp: 1525-1528,August2010.

[13] Wu, C. and W. Hsieh, 2000. "Digital watermarking using zero tree of DCT," IEEE Trans. Consumer Electronics , vol. 46, no. 1, pp: 87-94,April 2008.

[14]R.Manikandan, M. Uma, S M. MahalakshmiPreethi, "Reversible Data Hiding for Encrypted Image", Journal of computer Application ISSN: 0974-1925, Volume-5, Issue E1CA2012-1, February 10, 2012.

[15] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain,"*SignalProcessing:ImageCommun.*, vol. 26, no. 1, pp. 1–12, July 2011.

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

[17] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[18] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," *IEEE Trans.Inform.*

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue I, March 2015

Forensics Security, vol. 5, no. 1, pp. 180–187, Feb. 2010.

[19] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," *IEEE Trans. Inform. Forensics Security*, vol. 4, no. 1, pp. 86–97, Feb. 2009.

[20] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18,Jan 2007.

[21] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and Watermarking in video compression," *IEEE Trans. Circuits Syst. VideoTechnol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.

[22] R.Jose, G. Abraham, "A separable reversible data hiding in encrypted image with improved performance", Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy, 2013 Annual International conference on June 2013.

[23]C.Rengarajaswamy, K. Velmurugan, "Separable extraction of concealed data and compressed image", Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication system, Jan 2013.