International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue No. 12, December 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

STEGANOGRAPHY BASED MESSAGE HIDING IN IMAGE

S SrikanthNaik[1], P S V V N Chanukya[2]

[1]*Pursuing M.Tech (DIP) from Nalanda Institute of Engineering and Technology, Siddharth Nagar, Kantepudi Village, Satenepalli Mandal, Guntur dist, AP, (India)*

[2]*Working as Assistant Professor from Nalanda Institute of Engineering and Technology Siddharth Nagar, Kantepudi Village, Satenepalli Mandal, Guntur dist, AP, (India)*

ABSTRACT

Even though using digital communication batter secured communication is possible when compared to analogue communication still we are at risk while communicating with others using mobiles, systems etc. Secured information transformation can only possible when there is only information hiding or encoding which menace information is converted to other farm using separate key or algorithm. Without the algorithm received data is useless. Since the information transmitted can be detected there is a possibility to decode the data. In our proposed system we are hiding the data in the image instead of directly transmitting. Since the data we added is very less that person can't detect the changes he do not suspect that message hided in the image so that information is safe in the image. In digital image we are having a smallest units called pixels and which have a colour information. Out of all the images our information is hided in some pixels. Our pixels are hided in the image randomly and all this information is stored in the key. To produce low noise the image is converted to DWT which is well known as Discrete Wavelet Transform. After applying the DWT we are getting unnecessary pixels to hide the data.

I. INTRODUCTION

Information can be stored in two types which are digital and analogue, analogue is used in olden days andnow a days almost digital technology is used everywhere. That results in the easy transfer and easy access of data when compared to the analogue systems. Here the security plays major role when compared to other systems. In olden days cryptography is used which means data is encoded with the specific key so that the user only access the data because the only authorised user knows the key and even others accessed the he was unable to read the data because it is encoded. By way of the use of the net as a medium lots of data is transferred from one person to every other character. Every devicecan offer one-of-a-kind safety mechanisms for outgoing packets. The sender and receiver assures that there is records is securely transferred. but the records is transferred over covert (insecure) channel, if all people can get the encrypted data and via making use of cryptanalysis on it, the intruder can get the authentic message; the adversary can even regulate the records and skip to the receiver.It has some loop holes because the received one can read the data by applying some multiplications. It is possible to acquire the data from cryptography so a new improved technique is proposed such that in our system we can hide data

in an image without changing theimage visually, the person even watched the image cant realise data is included in the image which do not draw attention towards us which message is safe.

Instead of hiding the message directly we are hiding the message after applying the DWT which allow to more secure and also at the same time we can hide large amount of data when compared to other. The data in image can be hide in two ways which are image filters methods include DCT, DWT etc., and other is LSB which means Least Significant Bit. The last bit means the effect of last bit is very low when compared to LSB bit. Let see the pixel value be 85 decimal value. 85 can be represented in binary

0101 0101 - 85

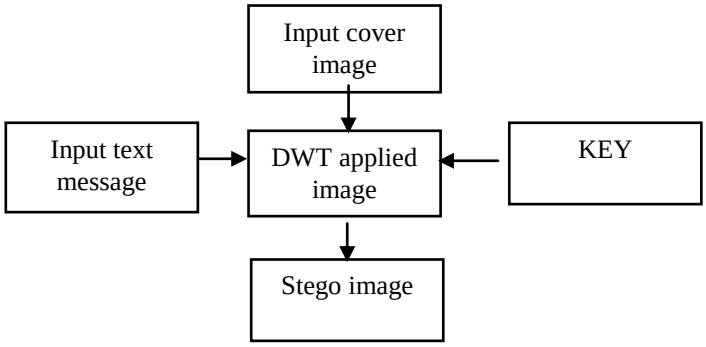
If we change the MSB value then the resultant output is 213 when compared to the bit valueand if we change the LSB value the resultant output is 84, which is very less and even cant noticeable. In LSB insertion we can see that the disturbance is from 85 to 84 which means one and while using the MSB bit insertion 84 is changed to 213 which means causing the disturbance of 129. So LSB insertion is preferred than the MSB insertion. We can change or insert LSB bits from one to four. According to our data we can insert from 1-bit LSB to 4-bit LSB insertion. If we use more than 4-bit means 5-bit or 6-bit the difference is widely visible which can draw the attention towards the picture. Since we are sending the low data which mince text file we are using 1-bit LSB insertion. The compressed text is now converted into its corresponding ASCII cost, in addition the ACSII is converted into its 8-bit binary cost. By way of using manage no longer gate, we are encoding the eight-bit binary price. Now these bits are prepared to embedded into an image using LSB insertion. The encrypted message is prepared to be embedded inside the cover image. Before embedding the message, the photo is now converted into its corresponding pixel values. Those values are arranged in the r x c matrix shape, r and c represent rows and columns respectively. The bit of the secret facts must be embedded within the random positions within the cowl photo. To discover the random positions, Random variety turbines acts like aces. Random numbers act like a key on this approach. Blum/shub generator and Pseudo random quantity generator are used to pick out the random rows and columns respectively. Random numbers are generated by way of the generator, the usage of the important thing (seed). Randomness can be various from generator to generator. The randomness is done by padding the bits in the series. After deciding on the random positions in the image (pixel values) now the name of the game message is embedded in the corresponding bits the usage of the LSB insertion method.

1101 0101 – 213	0101 0100 – 84
MSB changed value	LSB changed value

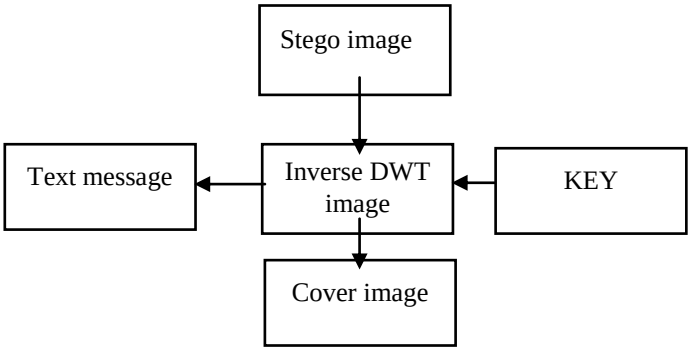
For security purpose we are creating the key which means the data stored pixels are stored in the data as key. Without the stored pixels it is impossible to find the message hided. Key is securely transmitted to the user such that the user at the other end can only see the data. With the help of the received key and the data the user can extract the message from the data and use the data. The brief description of the data is explained in below procedure. The total proposed method include two blocks which are embedding message and other is extracting message. Clear description is given in below tables. Discrete Cosine Transform and the Least Significant Bit insertion plays major role in our proposed system.

International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue No. 12, December 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

II. EMBEDDING SECTION



III. EXTRACTION SECTION



3.1 Discrete Wavelet Transforms

For each pair n, k of integers in Z, the Haar function $\psi_{n,k}$ ok is defined at the actual line R by using the system

$$\psi_{n,k}(t) = 2^{n/2}\psi(2^n t - k), \qquad t \epsilon R$$

This equation is suitable for right-open interval $I_{n,k} = (k\,2^{-n}, (k+1)\,2^{-n})$, i.e., it vanishes outside interval.

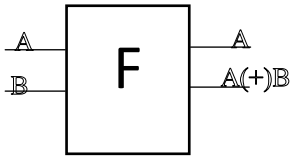
$$\int_R \psi_{n,k}(t)dt = 0, \qquad \|\psi_{n,k}\|^2_{L^2(R)} = \int_R \psi_{n,k}(t)^2 dt = 1$$

These functions are pairwise orthogonal

$$\int_R \psi_{n1,k1}(t)\psi_{n2,k2}(t)dt = \delta_{n1,n2}\delta_{k1,k2}$$

3.2 Least Significant Bit Insertion

Let consider some examples like insertion of bits to the data let take a character 'C' to embedded in the pixels and it take eight pixels data to hide in LSB bits. We are implementing CNOT gate to apply the embedding.



Let consider 'C' has ASCII value of 67 and in binary value of 01000011 and consider eight bits of data bits

10001000	10101101	10101101	11000101
11001101	11100111	10110011	00110011

Their original pixel values are changed to the corresponding output with the insertion of bit 'C'.

10001001	10101100	10101100	11000100
11110010	11100111	10110011	00110011

Due to the insertion of the data into the image there is some disturbances there are some differences in original and output image. To calculate the disturbances we are comparing the data of original image, output image, using the Mean Square Error and Peak Signal to Noise Ratio of an output image to estimate the noise of the image. Before reading an image as cover image if the image is colour image then the image is converted into the grey colour image since DWT is only applicable on two-dimensional systems instead of three-dimensional colour images. So only a grey colour image processed with the fixed size. The input image is resized to 800*800 so that uniform processing.Decryption is the repeal system of the encryption system. After receiving the stego picture, the receiver will convert the histograph into its corresponding pixels (matrix form). With the assist of key(seed) the receiver could be producing the random wide variety using the random mills to pick out in which positions the bits had been embedded. Upon getting the pixel positions, making use of opposite LSB insertion method will supply the encoded bits. Making use of the control now not gates at the encoded bits, the compressed textual content is retrieved. By applying wavelet, transformation approach (decompression) the authentic mystery data is retrieved.

The higher the Mean Square Error higher the noise, the higher the Peak Signal to Noise Ration lower the noise. Here are some calculations and experimental results with the MSE and PSNR are shown below

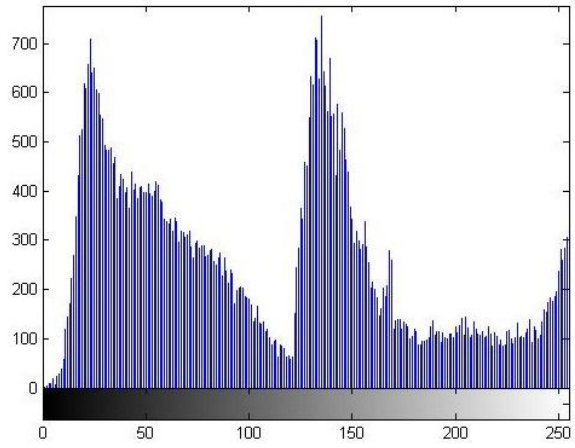
Noise type	Image one	Image two	Image Three	Image four	Image Five	Image Six
MSE	26.4896	40.6181	39.1456	45.5439	21.36	31.5887
PSNR	33.9	32.0436	32.204	31.5465	34.8348	33.1355

IV. RESULTS

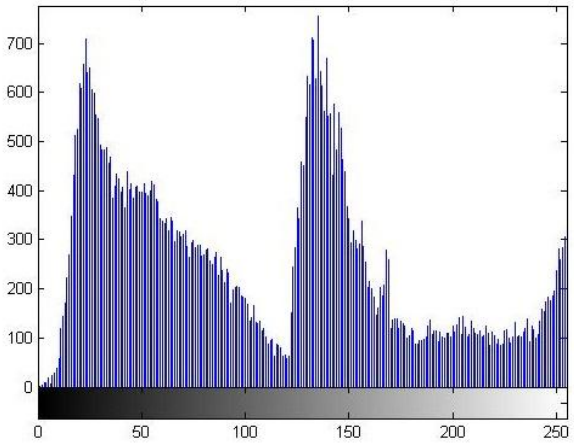
The input image which we considered for our operation is grey colour image instead of colour image because it is complicated to process the three-dimensional image instead of two-dimensional image.To process three dimensional image we have to extract three frames individually and apply 2-DWTwhich results in high noise ratio when compared to the two-dimensional image. Even though we considered colour image we convert image into grey colour image to avoid errors. The size of the grey colour image which means the height and width of the image is fixed or multiples of 8 such that it is easy to process. Then image is divided into small parts of size eight into eight (64 pixels in each block) and then processed through the image blocks instead of applying all the block at a time. We are applying individual blocks instead of whole image to reduce the noise. Since we applying DWT so that we can easily detect the noise pixels instead of inserting the message in the important pixels.Message is hided into to the noise pixels which results in low detection to Human Visual System which is in the low risk range.The message is inverse DWT is applied so that to retrieve the message. Message can't be retrieve without applying the inverse DWT. While using the secret key which is generated while inserting the message in the image we can extract the messaged from the cover image. Without the secret key we are unable to spot the secret pixels where we inserted the message. Inverse logics are applied at the time of the message extraction when the secret pixels are detected.

Input image considered as cover image **Output cover image after inserting message**

We can see in above images with low noise disturbances we are able embedded the message. Histogram for the two images are shown below. Histogram is the plot which is drawn to the intensity of pixel and no of the pixel.



Histogram of image one



Histogram of image two

Histogram of two images shown separately because the change is very less to notice due to LSB incursion of bits.

V. CONCLUSION

In our project we successfully hided the secret and valuable message in the image using the DWT and LSB insertion of the message in the image bits. The image bits those who hided are successfully extracted using the secret key which is generated while we are hiding the message in the image. The usage of LSB method,embedding big quantity of mystery facts in no longer possible. The primary idea of this paper is to embedded huge quantity of secret facts using LSB approach. To reap this primary the secret records is compressed the usage of wavelet transforms. After compression the bits are encoded the usage of a reversible quantum gate. LSB is one of the high-quality strategies when compared to transformation strategies, as it reduces masses of noise distortion. In cryptography, the intruder can recognise the existence of the message moving. Using this method big amount of statistics can be communicated inside the covert channel or even the lifestyles of the message is hard to pick out.

REFERENCES

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography", IEEE Seeurity and Privaey(3) pp. 32-44, 2003.

[2] R. C. Gonzalez and R. E. Woods, "Digital Image Processing", 2nd edition, Prentiee Hall, Inc, 2002.

[3] Venkatraman.S, Ajith Abraham, MarcinPaprzyeki, "Significance 0/ Steganography on Data Security", Proceedings of the International Conference on Information Teehnology: Coding and Computing (ITCC 04), ISBN: 0-7695-2108-8, IEEE 2004.

[4] Ivan W. Selesniek "Wavelet Transforms AQuiek Study", Physies Today magazine, October, 2007.

[5] S. Song, J. Zhang, X. Liao, J. Du and Q. Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Elsevier Ine, Advanced in Control Engineering and Information Science, Vol. 15, pp. 2767 - 2772, 2011.

[6] "Blum BlumShub", From Wikipedia, http://en.wikipedia.org/wiki/Bluffi_Bluffi_Shub"Controlled NOT gate", From Wikipedia, http://en, wikipedia . org/wiki/Controlled_NOT_gate .

[7] P. Marwaha and P. Marwaha, "Visual Cryptographic Steganography in Images", in Proe. ICCCNT, 2010, pp. 1-6.

[8] S. Song, J. Zhang, X. Liao, J. Du and Q. Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Elsevier Ine, Advanced in Control Engineering and Information Seienee, Vol. 15, pp. 2767 - 2772,2011.

[9] Changder. S, Ghosh. D, and Debnath. N.C, "LCS based text steganography through Indian Languages", in Proc. ICCSIT 2010, pp. 53-57.

[10] Juneja. M, Sandhu. P.S, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", ARTCom 2009, pp 302-305.

[11] Q. G. Mei, E. K. Wong and N. D. Memon "Data hiding in binary text documents", *Proc. SPIE*, vol. 4314, pp.369 -375 2001.

[12] Y.-C. Tseng, Y.-Y. Chen and H.-K. Pan "A secure data hiding scheme for binary images", *IEEE Trans. Commun.*, vol. 50, no. 8, pp.1227 -1231 2002.

[13] M. Wu and B. Liu "Data hiding in binary image for authentication and annotation", *IEEE Trans. Multimedia*, vol. 6, no. 4, pp.528 -538 2004.

[14] H. Yang and A. C. Kot "Pattern-based data hiding for binary image authentication by connectivity-preserving", *IEEE Trans. Multimedia*, vol. 9, no. 3, pp.475 -486 2007.

[15] H. Yang, A. C. Kot and S. Rahardja "Orthogonal data embedding for binary images in morphological transform domain¿¿¿A high-capacity approach", *IEEE Trans. Multimedia*, vol. 10, no. 3, pp.339 -351 2008.

[16] M. Guo and H. Zhang "High capacity data hiding for binary image authentication", *Proc. Int. Conf. Pattern Recognit.*, pp.1441 -1444.

[17] H. Cao and A. C. Kot "On establishing edge adaptive grid for bilevel image data hiding", *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp.1508 -1518 2013.

[18] T. Filler, J. Judas and J. J. Fridrich "Minimizing additive distortion in steganography using syndrome-trellis codes", *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp.920 -935 2011.

[19] T. Pevn¿¿, T. Filler, P. Bas, R. B¿¿hme, P. W. L. Fong and R. Safavi-Naini *Information Hiding*, vol. 6387, pp.161 -177 2010 :Springer-Verlag

[20] V. Holub and J. Fridrich "Designing steganographic distortion using directional filters", *Proc. IEEE Int. Workshop Inf. Forensics Security*, pp.234 -239.

[21] F. Huang, W. Luo, J. Huang and Y. Q. Shi "Distortion function designing for JPEG steganography with uncompressed side-image", *Proc. 1st ACM Workshop Inf. Hiding Multimedia Security*, pp.69 -76

AUTHOR DETAILS

	**S SRIKANTH NAIK,**pursuing M.Tech (DIP) from Nalanda Institute of Engineering and Technology, Siddharth Nagar, Kantepudi village, SatenepalliMandal, Guntur dist, AP, INDIA
	**P S V V N CHANUKYA,** working as Assistant Professor from Nalanda Institute of Engineering and Technology Siddharth Nagar, Kantepudi village, Satenepallimandal, Guntur dist, AP, INDIA