ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017

An Efficient Active and Passive Security Protection Method for Images

Drisya V P[1], Dr.Thajudin Ahamed V I[2] , Dr.Varun P Gopi[3]

PG Student [Communication and Signal Processing], Dept. of ECE, Government Engineering College, Wayanad, Kerala, India[1]

Professor, Dept. of ECE, Government Engineering College, Wayanad, Kerala, India[2]

Assistant Professor, Dept. of ECE, Government Engineering College, Wayanad, Kerala, India[3]

ABSTRACT: Highly extended multimedia data transfer through the communication channel is absolutely insecure.Therefor security protection measures are eminently essential. Such transmission of data need to be assured of security and consistency.In this paper offers integration of watermarking and encryption of independentlyfor grey scale images. Hence authentication can be verified even in the presence of decryption. In integration of encryption and watermarking technique Arnold transformbased encryption and watermarking technique based on discrete cosine transform is used. The experimental result shows that designed method do not decrease the quality of thegrey scale images which measured by means of peak signal to noise ratio. while integrating these two technologiesand also any type of watermarking technique and encryption can be used.This work also comparing various algoritms of proposed method.

KEYWORDS: Encryption, Watermarking, Orthogonal decomposition,

I.INTRODUCTION

Due to rapid growth in communication technology more and more data exchanges through internet are taking place. In multimedia applications images are transmitted through the communication medium. In computer based communication systems, network security is of outmost importance. At present, images of general interest that may contain sensitive information lacks efficient image security protection methods and such images are freely available from the internet. In business management and in government organisations, a large proportion of works is internet dependent and the security service requirement is quite high. With the development of digital device technology and the popularisation of Internet, the storage and distribution of multi-media information has become more and more appropriate. But the security of digital multi-media information attracts more people's attention.

Encryption is the active technique for guaranteeing the privacy of the pictures and it converts picture into some irreversible form. Authentication protects against unauthorized user access this may leads hiding some data or image into the original image.This leads to watermarking which is a passive method. Both methods have some drawbacks. The most notable thing is that the image is in plain text during the process of extracting passive security information and this is a greater threat for the security of carriers. At times, the owner would not want to reveal the details of carrier, for example: a third party inspection, and request for the direct extraction of passive protection information from ciphertext. Although, the second method avoids the shortcomings of first one, its drawback is obvious: embedding of passive protection information in ciphertext makes the carrier's data change and the change may cause the key information to become unrecoverable. In order to avoid this, the change of ciphertext must be recovered. In such cases, the plain text will be without passive protection. Both encryption and marking technology offers security by modifying carrier data, and direct superposition causes interference with each other. To avoid the mutual interference between encryption and mark embedding, integration of encryption and marking technology is done based on orthogonal decomposition.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017

Recently certain methods have been developed to integrate encryption and watermarking for protecting digital images, which can guarantee security. This algorithm takes advantage of the feature of spatial scrambling in only disordering the arrangement of protected data, which essentially would not disturb the embedding of watermark by modifying carrier data, to achieve the integration of en-cryption and watermarking. However, this integration algorithm is only available for spatial scrambling. proposed a method to integrate encryption and watermarking by embedding mark with the decrypting simultaneously, which took advantage of the slight difference between encryption key and decryption key to gain an imperceptibly different plain text to achieve mark embedding. However, for the remote sensing images, this method provides only one kind of security protection at a time.Hence the encrypted remote sensing image doesn't bear the watermark and the watermarked image will be visible to everybody.

II.PROPOSED METHOD

Literature survey is the first method of proposed method .It uses the benefits of discrete cosinetransform, Arnold Transform and Chaoss. Two security strategies are utilized to improve the prottection of the image which are transmitted through awgn channel.Also comparing theperfomance of different algorithms.

a. Discrete cosine transform

The most popular technique for image compression, over the past several years, was Discrete cosine transform (DCT). Its selection as the standard for JPEG is One of the major reasons for its popularity. DCT is used by many Non-analytical applications such as image processing and signal-processing DSP applications such as video conferencing. The DCT is used in transformation for data compression. DCT is an orthogonal transform, which has a fixed set of basis function.Dct is used to map an image space into a frequency DCT has many advantages: It has the ability to pack energy in the lower frequencies for image data.It has the ability to reduce the blocking artefact effect and this effect results from the boundaries between sub-images become visible.

b. Slant transform

A unitary transform specifically designed for image coding. The transformation possesses a discrete sawtoothlike basis vector which efficiently represents linear brightness variations along an image line. A fast computational algorithm has been found for the transformation. The slant transformation has been utilized in several transform image-coding systems for monochrome and color images. Computer simulation results indicate that good quality coding can be accomplished with about 1 to 2 bits/pixel for monochrome images and 2 to 3 bits/pixel for color images.

$$S_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$S_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ a_2 & b_2 & -a_2 & b_2 \\ 0 & 1 & 0 & -1 \\ -b_2 & a_2 & b_2 & a_2 \end{bmatrix}\begin{bmatrix} S_1 & 0_2 \\ 0_2 & S_1 \end{bmatrix}$$

c. Arnold Transform

Proposed method exploits the property of Arnold transform based encryption. Digital image scrambling can convert image into a completely different meaningless image during transformation.Chaotic image after scrambling encryption algorithms available. so attacker cannot decipher it. Due to very well mathematic characteristics of Arnold scrambling algorithm it is widely used . Arnold scrambling recovery has two ways: one is the application of its periodicity, and the other is the pursuit of its inverse matrix to the inverse transformation. It is very natural to leverage the periodicity of Arnold scrambling method. Previous studies have led to the following conclusion for the digital image of size N X N pixels the Arnold scrambling has periodicity. However, the times of scrambling are related to the order of N,when we used its periodicity to get the anti-Arnold transformation algorithm, especially when it used in the picture with big

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017

degree waste a lots of time. In the case of picture with big degree mainly depending on the inverse matrix to the Arnold scrambling recovery.The transformation by using Arnold transform of (x,y) coordinate and its periodicity given below

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \text{ Mod N}$$

Size of image(N)	Cycle of scramblin(T)	Size of image(N)	Cycle of scrambling (T)
3	4	25	50
4	3	32	24
5	10	64	49
6	12	100	150
7	8	120	60

d. Orthogonal decomposition

Orthogonal transform presented in the proposed design is for the operation independence and the joining the information of encryption and watermarking technique. The key of orthogonal transform is the matrix B,B implies different orthogonal transform. In the principle image different orthogonal transforms can be applied.Orthogonal transform consisting Fourier transform, cosine transform, and wavelet transform, and each has its extraordinary qualities. The vectors of B are common orthogonal, then the modification
of transform coefficients would not scratch off each other in the first data space, which
implies that the modification impact of transform coefficients is simply related with
the modification amount yet not the modification location, It is significant thatdiscrete cosine
transform is an extraordinary finish orthogonal transform and also along these lines, Walsh transform is more appropriate.for computerized flag handling and more advantageous for Pc. its transform
matrix is made out of +1 and -1.

d. Integration of Watermark embedding- Encryption algorithm

1. Take the original image and resize it to 256 X 256 image. Preprocessed by using Dct
2. Take the watermark and resize it to 32X32 bit grey scale image. .
3. Then apply the Arnold transformation to the loaded image.
4. After the Arnold transformation to the image , apply Dct to the watermark.
5. Perform the embedding of the watermark in the original image
6. Take the inverse DCT to get the encrypted-watermarked image

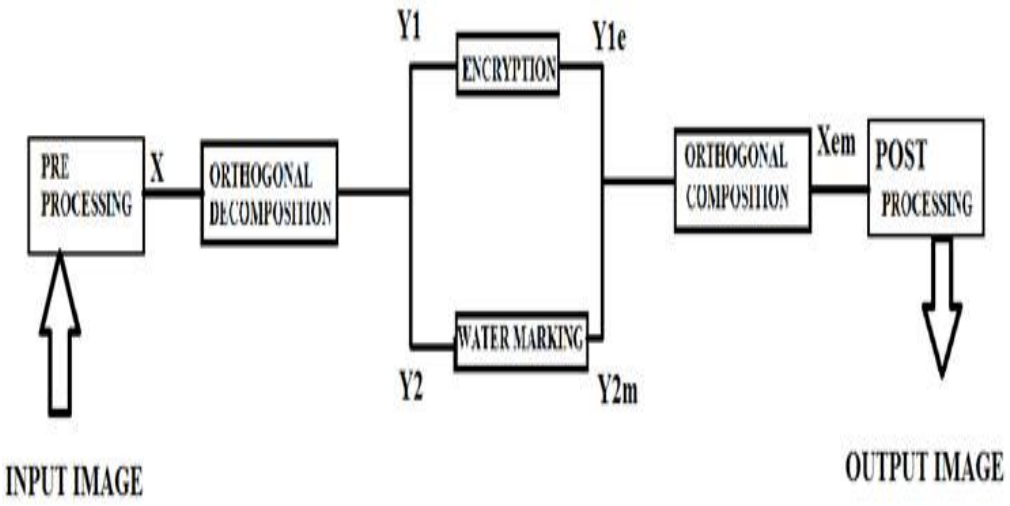
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017



e. Watermarking Extraction and decryption algorithm

The flow chart for watermarking extraction and decryption algorithm is shown in figure 3.The steps involved in extraction algorithm are given below

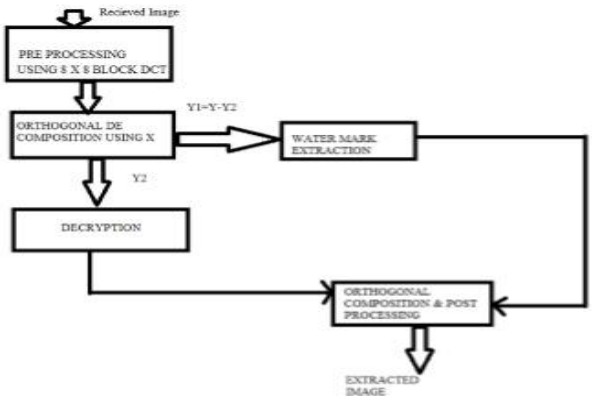
1. Take the watermarked image and resize it to 256X 256 image.

2. Then take the DCT .

3. Extract the watermark from high frequency component.

4. Take the inverse DCT transformation of the extracted watermark to get the desired extracted watermark.

5. Take the inverse Arnold transformation of the image .



Recent researches that aiming at merging encryption and Watermark are divided into three strands: transmitter side encryption and Watermark embedding, transmitter-side encryption and receiver Watermark embedding, joint Watermarking and decryption. Transmitter side watermark embedding involves fingerprinting at the source, then encrypting and transmitting it. This scheme should generate n different fingerprinted copies for n users first, then encrypt and transmit it respectively. This approach has poor scalability because for large number of users, data processing efficiency lowers while the bandwidth and overhead of data transmittion are high. Receiver-side watermark

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017

embedding encrypts data at source, decrypts and embeds watermark at receiver side by reliable tamper-proof hardware, . The disadvantage with this method is that its security lays on extra hardware or reliable client, making it an impractical solution. Another solution is integrating decryption and fingerprinting process. Anderson proposed a method to encrypt plain text audio data using one key, and different users decrypting ciphertext by slightly different keys, so that each user gets a slightly different LSB of audio data. But this scheme is inefficient because raw audio format is encrypted instead of compressed form. The scheme is also vulnerable to collusion. In this scheme, The whole process is divided in to four sections. The first section consists of generation of embedding mark. According to the practical application, owner can construct the embedding mark with copyright information. The second section includes some pre-processing steps. The input image is divided in to block of 8X8 sub images. After 8X8 block-DCT, data quantization, and DCs differential encoding, all nonzero coefficients of the host image contribute the operation dataset. Next section includes encryption and watermarking based on orthogonal decomposition. In the post-processing stage , the encrypted and watermarked coefficient set is multiplied with orthogonal decomposition matrix to obtain the encrypted and watermarked image.Watermark is controlled by a key ,here changing the domain from spatial domain to frequency domain of watermark which can be recovered by the owner in the reciever side

IV. PERFOMANCE EVALUATION

The terminology PSNR generally used for expressing the relation of the peak signal to noise power of the signal into the noise power which affects the signal. Dynamic range of the Peak signal to noise ratio is high usually it represented in decibel logarithmic scale.Generally, PSNR is used to measure the quality of reconstruction of lossy image compression. In this case, the signal is the original data, and the error introduced as a result of compression is the noise . It is actually human perception of reconstruction quality and peak signal to noise ratio value means quality is higher. The possible value range of metric is important.Comparison of different metric values of same images are essential. PSNR is defined as the mean squared error (MSE). For a noise-free m × n monochrome image I and noisy image K, MSE is defined as

$$mse = 1/(mn)\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}[I(i,j)-k(i,j)]^2 \qquad psnr = 10 * log((255^2)/mse)$$

The following table shows the evaluation result for different images .Here is the comparison of the two algorithms.Algorithm based on Dct and algorithm based on DWT[10]

IMAGE	PROPOSED METHOD PSNR	ALGORITHM BASED ON DWT-PSNR
Lena .JPG	42	40.44 0 0
Cameraman.tif	40	40.43 0 0
Peppers.png	42	40.47

The following graph shows the evaluation result for different images .Here is the comparison of the two algorithms.Algorithm 1 based on Dct and algorithm 2 based on slant transform.

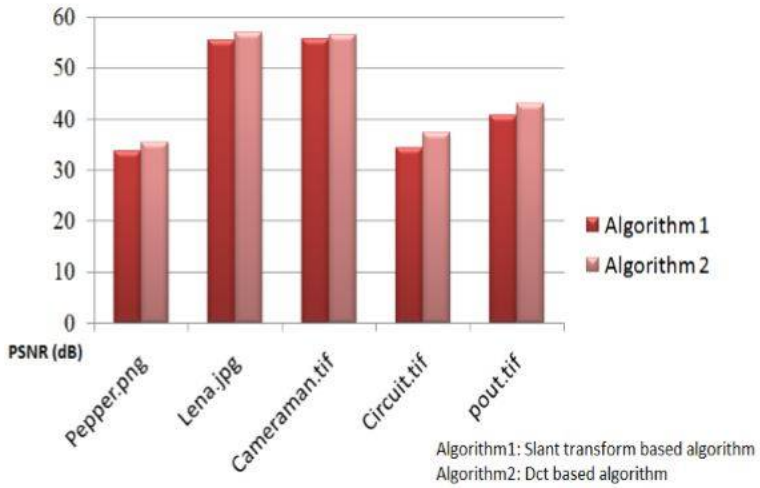
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

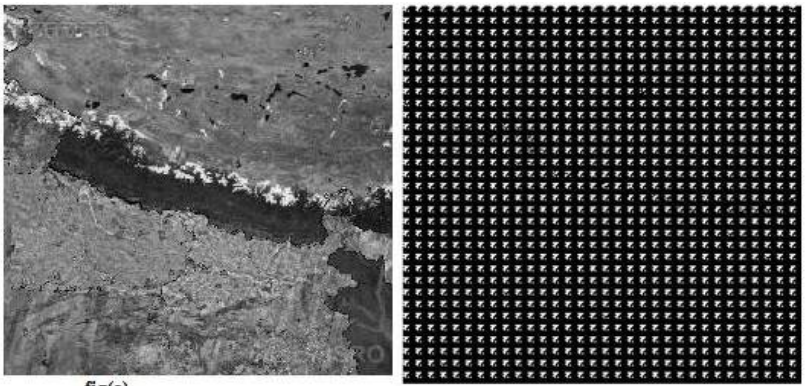
(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017



In Walsh Hadamard transform based algorithm,The PSNRs of the 10 decrypted-marked are all around 35 dB. The decrypted-marked remotesensing image whose PSNR=38.86dB [1].But in Proposed Dct based algorithm ,fig(a)is the remotesensing image collected from NRSC bhuvan website.fig(b)is the encrypted water marked image using orthogonal decomposition,fig(c)extracted image whose PSNR =40.7 dB. Compared to the original image, there is little difference and the proposedalgorithm satisfies the marking invisibility constraint.



fig(a)

fig(b)

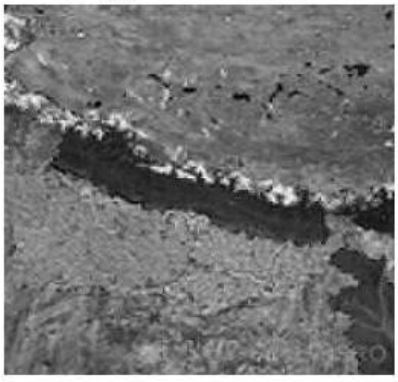


fig (c)

WATERMARK OF THE SYSTEM

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

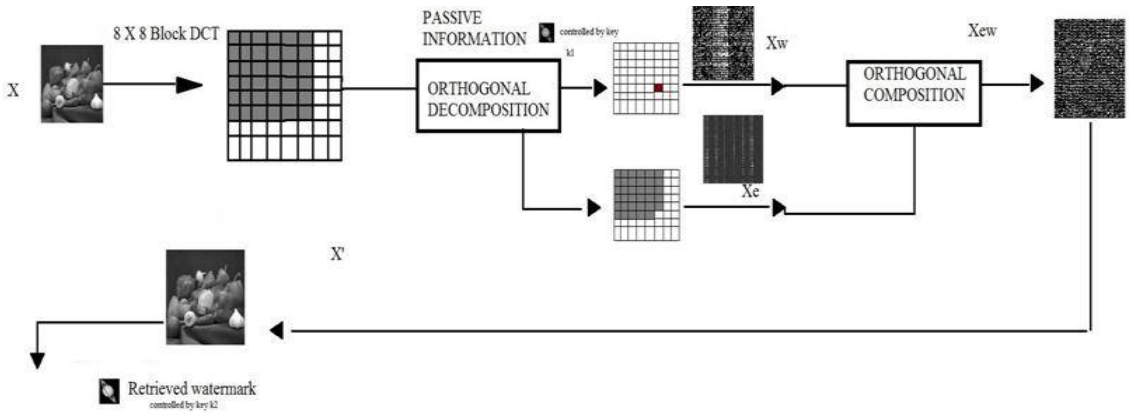
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 7, July 2017

Figure given below is the result of the experiment. All these algorithms are simulated in MATLAB . The PSNR is used to evaluate the performance of presented approach for the selection of appropriate algorithm. It is found that proposed method can be used instead of existing methods.



VI.CONCLUSION

The primary goal of the present work was to develop a method for the secure transmission of images. There are di□erent techniques to give comprehensive protection for image separately. It is proposed that integrating di□erent technologies gives better result. Preprocessed (with DCT) images were successfully decomposed orthogonally the with the help of orthogonal transforms. The two technologies of encryption and watermarking were integrated independently into the same image and any type of encryption and watermarking technology can be applied. The experimental data supported our hypothesis- on analysis it was found that proposed method maintained the quality of retrieved image. Experiments on collected data set show that quality of the image did not degrade by integrating encryption and watermarking. Images of general interest, remote sensing data etc are to be protected during image transfer. On comparison with other methods, it was observed that better performance in terms of image quality was achieved by this new approach. Performance of the proposed method highly depends on the transform that is used for orthonal decomposition and preprocessing. Apropriate transforms which gives better result has to be chosen by the observing changes in the result. In the case of remote sensing data quality improvement of images are essential, so better transforms have to be used to improve the performance

REFERENCES

[1] Zhengquan Xu Li Jiang, Tianye Niu and Yanyan Xu. "Integrating Encryption and Marking for Remote sensing image Based on Orthogonal Decomposition". Applied Earth Observations and Remote Sensing, IEEE Journal, 8(issue :5), AUGUST 2015.
[2] Zhengquan Xu Li Jiang, Tianye Niu and Yanyan Xu. "A New Comprehensive Security Protection For Remote sensing Image based on the integration of encryption and watermarking". Geoscience and Remote SensingSymposium(IGARSS), (5).
[3] G.Strang. "introduction to linear algebra, 4th ed". Cambridge,MA, USA: Wellesley-Cambridge, (4).
[4] Zhengquan Xu Li Jiang, Tianye Niu and Yanyan Xu. "commutative encryption and watermarking for remote sensing image". Int. J. Digit. Content Technol, 6(4).
[5] B. Chen and G. W. Womell. "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding". IEEE Trans. Inf. Theory, 47.
[6] G.Strang. "introduction to linear algebra, 4th ed". Cambridge,MA, USA: Wellesley-Cambridge, (4).
[7] Anil K Jain. Digital image processing". PRENTICE HALL, 1989.
[8] Rajesh CheriM Ro) and R. Gopilakumari. "A new transform tor 2-d signal represen-lation (mrt) and some of its properties". IEEE, 2004.
[9] R. C. Gonzales and R. E. Woods, Digital Image Processing, 3rd ed.Englewood Cliffs, NJ, USA: Prentice-Hall, 2007, pp. 558–563.
[10] Gusharanjeet Singh Kalra, Rajneesh Talwar, Harsh Sadawarti "Robust Blind Digital Image Watermarking Using DWT and Dual Encryption Technique"
[11] M. Barni, F. Bartolini, V. Cappellini, E. Magli, and G. Olmo, "Near-lossless digital watermarking for copyright protection of remotely sensed images," in Proc. IEEE Int. Geosci. Remote Sens. Symp. (IGARSS), 2002, vol. 3, pp. 1447–1449.
[12] B. Chen and G. W. Womell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1423–1443, May2011