International Journal of Research in Advent Technology, Vol.2, No.3, March 2014

E-ISSN: 2321-9637

Cognitive Spread Spectrum Crypto Data Transformation Using OFDM for Improved SNR

Revathi V[1], Dhanasekar N E[2], Vinothkumar S[3], Sasikumar M[4]
Department of ECE[1, 2, 3, 4], Aksheyaa College of Engineering[1, 3, 4], St Peter's University[2]
Email: eng.revathi89@gmail.com[1]

Abstract-The most common problem occurs when sending the data from one person to another person due to security problem like hacking the data by tracking the password by third party. So everything will be lost by the user. The proposed system consists of public key cryptography technology. In that, we will implement the communication process through RSA algorithm. Here we take two images (Cover image and secret image). Digital media is nothing but an image, audio, video; here the cover image will act as a digital media. Further, the secret image is embedded with the cover image using two dimensional Discrete Wavelet Transform (DWT) in the presence of spread spectrum carrier.

Index Terms: Digital media, Spread spectrum carrier, Cryptography

1. .INTRODUCTION

An information technology field of rapidly growing national security interest uses digital data embedding in digital media. Other applications like medical field, military uses secret communication between trusting parties. In this project the secondary data are embedded to the primary data with addition of additive white Gaussian noise. Spread spectrum involves a adding of noise to the object. The noise adding technology gives good modulation scheme at the receiving end. In sender side, our aim is to hide secret image to the cover image (the secret image is already mixed with noise by spread spectrum) after that we put a encryption key to produce the crypto image. The secret image is not transparent to any one without giving correct decryption key. At the other end, thereby giving correct decryption key it will be extracted by user. The basic attributes of data hiding is follows,

- Security – Not able to access the communication channel by unauthorized party.
- Robustness – Tolerance of hidden data to noise or any other disturbances.
- Payload – Delivery rate about data.
- Transparency – Low host distortion for concealment purposes.

Latest, making data embedding technologies are being seen to cause a threat to personal privacy, commercial and national security interest. In this work, we focus our attention on the blind recovery of secret data hidden in medium hosts via spread spectrum transform domain embedding. This blind hidden data extraction problem has also been referred to as "Watermarked content Only Attack" (WOA) in the watermarking security context.

2. OFDM-IDMA SYSTEM MODEL

The bit error rate performance of interleave division multiple access (IDMA) based systems can be predicted by signal to-noise ratio (SNR) evolution which tracks the average symbol SNR at each iteration and provides a faster solution than brute force simulations. Orthogonal frequency division multiplexing interleave division multiple access (OFDM-IDMA) is a promising multiple access scheme for uplink wireless communications due to its potential of achieving high spectral efficiency and low decoding complexity. In OFDM-IDMA systems, users are separated by distinct interleaves and the receiver removes the multiple access interference (MAI) for each user using an iterative chip by-chip detection algorithm.

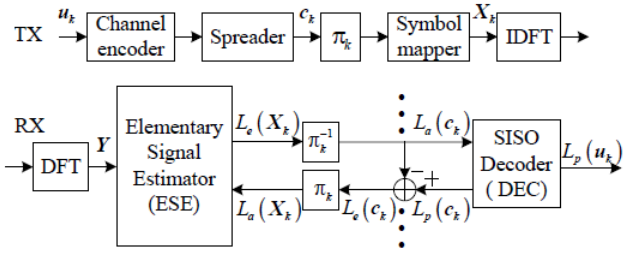

Fig 1: OFDM-IDMA transmitter for user-k and receiver.

The above fig shows the transmitter for user-*k* and the receiver. At the transmitter, information bits ***u****k* are first encoded and then spread by a length-*S* spreader. The bits ***c****k* (*}*1) after spreading are referred to as *chips*. The chips are interleaved by a random *user-specific* interleave *πk* and then modulated using quadrature phase shift keying (QPSK), giving rise to the modulated symbols which are finally transmitted on the *N* subcarriers via an inverse discrete Fourier transform (IDFT) module. The receiver mainly consists of two modules, *i.e.*, the elementary signal estimator (ESE) for all users and the soft-input soft-output decoders (SISO DECs) for each and every user.

The key idea of SNR evolution is to treat the MAI as noise such that the BER performance in a

multiuser scenario is approximated by a single user scenario with a specific SNR which is updated at each iteration. As it is difficult to obtain the exact value of the SNR in the evolution process, an approximate SNR updating formula has been proposed.

3. BLOCK DIAGRAM

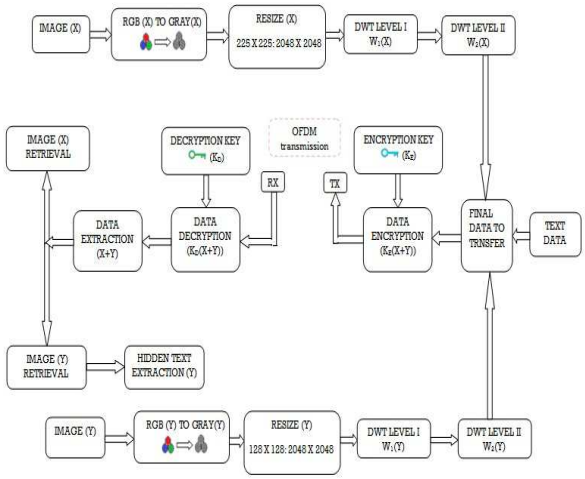

Fig 2: Block diagram

The general process of image watermarking is shown in Figure 2. The original image is modified using the signature data to form the watermarked image. In this process, some distortion may be introduced. The extraction process may or may not require the knowledge of the original image for getting back the hidden signature. The extracted watermark is then compared with the original signature; the difference must be as low as possible. A Discrete Wavelet Transform is used to hide the image in pixel by pixel at Z – axis. Spread spectrum in image treat the cover image as noise or by adding pseudo-noise to the cover image.

The Bit Error Rate or bit error ratio (BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval.

The formula for calculating PSNR is,

$$\text{PSNR} = 10.\log_{10}\left(\frac{\text{MAX}_\text{I}^2}{\text{MSE}}\right) \ldots\text{Eq. (1)}$$

$$= 20.\log_{10}\left(\frac{\text{MAX}_\text{I}}{\sqrt{\text{MSE}}}\right)$$

$$\text{PSNR (dB)} = 20 \text{ . } \log(\text{MAX}_\text{I}) - 10.\log(\text{MSE})$$

The formula for Mean-Square error is

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

where,

m: width of image.
n : height.
m*n: number of pixels

3.1. *Additive white Gaussian noise*

Additive White Gaussian Noise (AWGN) is a channel model in which the only impairment to communication is a linear addition of wideband or white noise with a constant spectral density (expressed as watts per hertz of bandwidth) and a Gaussian distribution of amplitude. The model does not account for fading, frequency selectivity, interference, nonline arity or dispersion. AWGN is commonly used to simulate background noise of the channel under study, in addition to multipath, terrain blocking, interference, ground clutter and self interference that modern radio systems encounter in terrestrial operation.

3.2. *Discrete Wavelet Transform*

The basic idea of Discrete Wavelet Transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district. Then transform the coefficient of sub-image.

After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one Low-Frequency District (LL) and three high-frequency districts (LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. . A two-dimensional image after three-times DWT decomposed can be shown as Fig.3.

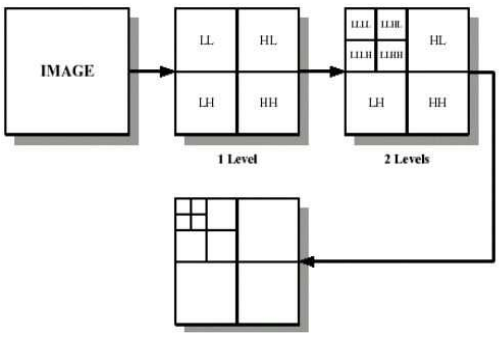

Fig 3: Example of DWT

3.3. *Image Encryption*

Initially take two images such as shown in Figure 4 and 5. One is cover image (Original image) that it is the medium for hidden image. And then encrypt our secret image with cover image in-order to get the encrypted image using relevant encryption algorithm. Here we are using 2 Dimensional Discrete

Wavelet Transform (2D-DWT) algorithms for encryption.

Fig 4: Original or Cover Image

Fig 5: Secret Image

. Generally, the wavelet transform can be expressed by the following equation:

$$F(a,b) = \int_{-\infty}^{\infty} f(x)\psi^*_{(a,b)}(x)\,dx \ldots\ldots \text{Eq. (3)}$$

Where the * is the complex conjugate symbol and function ψ is some function. This function can be chosen arbitrarily provided that obeys certain rules.

Property	**2D DCT**	**Wavelet transform**
Image intensity	98.16%	96.4%
MSE in dB	8	10
Execution time	3.8	0.9
Compression	0.025	8.5

Table 1 : Comparison results produced between DCT and DWT

3.4. *Generation of Encrypted Image*

It has pair of keys one is public key (which is known by both sender & receiver) and another one is private key (which is known only by the receiver).The Asymmetric key algorithm is used for encrypt the image by giving public key. In transmitter side they kept their private key in secret.

The RSA Algorithm,

1. Bob chooses secret primes p and q and computes n = pq.
2. Bob chooses e with (e,(p – 1) (q − 1)) = 1.
3. Bob computes d with de = 1 (mod(p − 1)(q − 1)).
4. Bob makes n and e public and keeps p, q, d secret.
5. Alice encrypts m as $c \equiv m^e \pmod{n}$ and sends c to Bob.
6. Bob decrypts by computing $m \equiv c^d \pmod{n}$.

4. EXPERIMENTAL OUTPUT:

Fig 6(a) : Fused image final

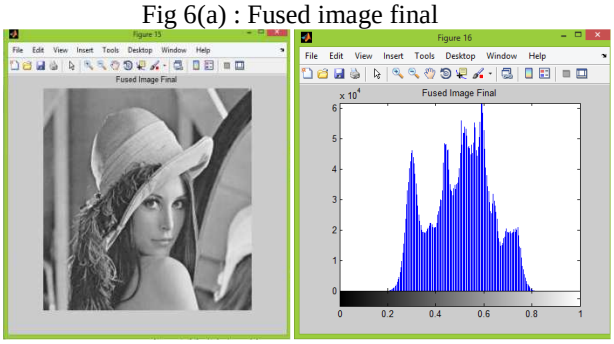

Fig 6(b) : Private key generation for encryption

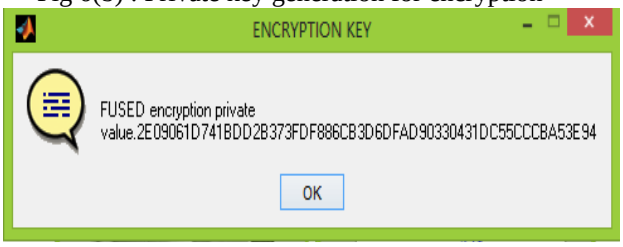

Fig 6(c) : Extraction of secret image from cover image

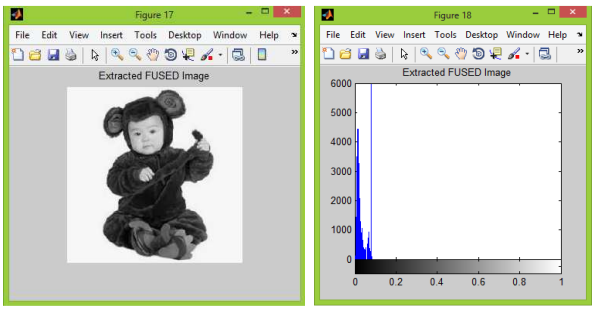

Fig 6(d) : Private key for decryption

Conclusion and Future Enhancement

The main goal of my project was embedding of one image into other image in presence of noise

as a case of steganography. The two primary criteria for successful steganography are that the stego signal resulting from embedding is perceptually indistinguishable from the host image signal, and the embedded image is recovered correctly at the receiver. The future extension of my project will makes hiding texts into image. There too reducing probability of errors occurring in image extraction and restoration. There by giving detailed experimental studies can be taken up for a later stage to proceed. The improved PSNR value about 50dB.

Acknowledgement

The authors would like to thank the reviewers for a wealth of suggestions and comments that helped to improve the presentation and content of this manuscript.

Citations

Zhenxing Chen; Eun Chang Choi; Seog Geun Kang "Closed-form expressions for the symbol error probability of 3-D OFDM", *Communications Letters, IEEE*, On page(s): 112 - 114 Volume: 14, Issue: 2, February 2010.

Seog Geun Kang; Zhenxing Chen; Ju Yeong Kim; Jin Sub Bae; Jong-Soo Lim "Construction of Higher-Level 3-D Signal Constellations and Their Accurate Symbol Error Probabilities in AWGN", *Signal Processing, IEEE Transactions on*, On page(s): 6267 - 6272 Volume: 59, Issue: 12, Dec. 2011.

Zhenxing Chen; Seog Geun Kang "Probability of symbol error of OFDM system with 3-Dimensional signal constellations", *Consumer Electronics, 2009. ISCE '09. IEEE 13th International Symposium on*, On page(s): 442 – 446.

Dehghani, M.J.; Jafarian, N.; Kazemi, K. "Peak-to-Average Power Ratio in 3-D OFDM system", *Telecommunications Forum (TELFOR), 2012 20th*, On page(s): 475 – 477.

Zijing Zhang; Eun Chang Choi; Seog Geun Kang "Trellis coded 3-dimensional OFDM system", *Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on*,On page(s): 1106 – 1109.

References

[1] Cachin .C, "An information-theoretic model for steganography," in Proc. 2nd Int. Workshop on Information Hiding, Portland, OR, USA, Apr. 1998, pp. 306–318.

[2] Gul .G and Kurugollu .K, "SVD-based universal spatial domain image steganalysis," IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 349–353, Jun. 2010.

[3] Hartung .F and Kutter .M, "Multimedia watermarking techniques," Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information, vol. 87, pp. 1079–1107, Jul. 1999.

[4] Malvar .H.S and Florencio .D.A, "Improved spread spectrum: A new modulation technique for robust watermarking," IEEE Trans. Signal Proc., vol. 51, no. 4, pp. 898–905, Apr. 2003.

[5] Meyer C.D, Matrix Analysis and Applied Linear Algebra. Philadelphia, PA, USA: SIAM, 2000.

[6] Petitcolas .F.A.P, Anderson R.J, and Kuhn .M.G, "Information hiding: A survey," Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[7] Qiang .C and Huang T.S, "An additive approach to transform-domain information hiding and optimum detection structure," IEEE Trans. Multimedia, vol. 3, no. 3, pp. 273–284, Sep. 2001.

[8] Valizadeh. A and Wang .Z.J, "Correlation-and-bit-aware spread spectrum embedding for data hiding," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 267–282, Jun. 2011