VOL. 10, NO. 6, APRIL 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

AN AMALGAMATED APPROACH OF CRYPTOGRAPHY AND STEGANOGRAPHY USING IWT AND RANDOM PIXEL SELECTION FOR SECURE TRANSMISSION

V. Vaithiyanathan, B. Karthikeyan, Anishin Raj M. M., M. Rajasekhar Reddy, Priyanka S. and K. Abinaya
School of Computing, SASTRA University, Thanjavur, India
E-Mail: mbalakarthi@gmail.com

ABSTRACT

Steganography is the art of concealing the message such that even the cyber geeks do not suspect the existence of the message. Cryptography is the technique of secret writing especially in the form of code and cipher systems but the presence of message is known. This paper, presents a secured data transformation by blending Steganography and cryptographic techniques together to improve the standard of data security such that none other than the intender and the receiver will be able to extract the proper data. The integer wavelet transformation is used to transform the data into an unintelligible format. Transformed data are embedded using least significant bit substitution into the cover image. The intensity of the pixel range which is frequent in image is selected and infixing of data is done on this selected range of pixels. This process is also reversible. This improves the efficiency in secured transmission as it approaches different patterns each time the same data embedded in different images. This algorithm can be best utilized to encrypt passwords and keys which are transmitted by 3rd party. It can also be considered to store digital signatures in the database.

Keywords: steganography, cryptography, integer wavelet transform.

INTRODUCTION

Developing effective secured systems across two dealers to transmit the data secretly is one of the most required techniques worldwide. Each data around the world has been digitalized for data maintenance, retrieval and efficient storage. But the data transmitted across, is being hacked by the intruder. Even though several methods and techniques have been used by the service providers, possibility of security breech still exists (Ajit Singh *et al*., 2013; Shilpa Sunil Wankade *et al*., 2013). Focusing on the advanced techniques of data security, this paper is being implemented on steganography (M. Padmaa *et al*., 2014). Here the secret information is embedded into an image which will be transmitted to the receiver. Data being hidden in the image, none other than the sender and the receiver is aware of the existence of the data (Amirtharajan *et al*., 2012). Infixing of data into the pixel has been done on the basis of pixel selection using particular criteria (B. Elangovan *et al.,* 2013). This paradigm considers pixel intensity of certain range. Due to this criterion, culling of pixels depends on the image, which is carried away by positional variance of the pixel. This results in uniqueness in embedding process, as insertion of data depends on the image in which it is inserted. This sets a hindrance to the cryptanalysis to determine the track of embedding technique. Invariably, implementation of this technique is easier since the only criterion put upon is judgment of pixels within certain range.

To enhance the system of data security, cryptography is also implemented on the hidden message (Manikandan *et al*., 2011). Cryptography is a technique which transforms the data into unintelligible format. Several transformations could be applied on the data to make it more secured. In any discretized transformations, wavelet transformation (Po-Yueh Chen *et al*., 2006) is considered to be one of the most popular candidates among time-frequency transformations, which are oscillations that start at zero, increase, and then decrease again to zero. As a mathematical tool, wavelets can also be used to represent data and to extract information from different kinds of sources, not restricted to audio signals and images. Wavelet transform can be broadly classified into three classes: continuous, discrete and mutli-resolution based.

Continuous wavelet transforms are subjected to uncertainity principle of fourier analysis. For a given event in a signal, one can find it difficult to assign simultaneously exact frequency and time scale to that event. It results in mapping of entire scale map instead of just a point. In discrete wavelet wavelet transformation, the signals are discretely sampled. Unlike fourier transformation, it can capture both location information and frequency.

The wavelet series can be represented as square-integrable function by certain orthonormal series. A function can be defined as orthonormal function if it is completely defined by orthonormal system, i.e. $\varphi \in L^2(R)$

The complete orthonormal system is defined by Hilbert basis

$$\varphi_{jk}(x) = 2^{\frac{j}{2}}\varphi(2^j x - k)$$

For integers $j, k \in Z$

The integral wavelet transformation is defined as

$$[W_\varphi f](a,b) = \frac{1}{\sqrt{|a|}}\int_{-\infty}^{\infty} \overline{\varphi\left(\frac{x-b}{a}\right)} f(x)dx$$

where a and b are scaling and time factor respectively.

The basic idea behind wavelet is that the changes should be applied in time extension, not on the shape of signal. Based on the uncertainty principle of signal processing, the extension in time is expected to have considerable change in frequency domain.

$$\Delta t * \Delta \omega \geq \frac{1}{2}$$

Where t is time factor and ω is frequency.

Wavelet compression is the methodology behind the data compression using wavelet transformation (L. Yang *et al*., 2013; V. Thanikaiselvan *et al*., 2011; A. De Vos., *et al*., 2012). This produces coefficients for each of the data value and is considered to be more effective as the coefficients are concentrated to reduce the complexity in conversion. A set of complementary process is carried out without any gaps or overlaps so that the original signal can be regained. The compression/ decompression techniques have been used together to regain the data with minimal loss. There are only few finite number of wavelet coefficients for each regularly bounded regions within the specified half plains. This theoretical analysis of transformation concludes in the lossy transformation due to the decompression of the real numbers, which results in deviation of the value to certain level. To reduce the amount of complexity in the numerical calculation, the transformed value is restricted to an integer, which is Integer Wavelet Transformation (IWT). An IWT based approach for steganography is proposed (Ramalingam *et al*., 2014) for the reconfigurable hardware.

The IWT (B. Ramalingam *et al*., 2014) is basically a modification of linear transformation. The transformed value is being rounded to the nearest integer. The advantageous part of integer wavelet transformation is that the lossless compression is achieved and memory is reduced as integers are considered instead of the real numbers. Integer wavelet transform can be expressed as discrete wavelet transform added to a certain rounding noise. The next level is enclosure of transformed data into the cover image. Least significant bit (C.K. Chan *et al*., 2003; C.C. Chang *et al*., 2000; B. Mahboob *et al*., 2008; S. Mukherjee *et al*., 2012; Tao Zhang *et al*., 2010; C.H. Yang *et al*., 2008; Young-Ran Park *et al*., 2005) is the most effective embedding methodology used in steganalysis in which bit transformation is carried out by replacing the least significant bit of the image pixel with data bit. The error due to the secret data bit is very low due to the induced data bit may produce a change of at most one bit. This reduces the MSE value of the image.

MATERIALS AND METHODS

This is to evaluate different techniques and algorithms being implemented and helps us to analyze the efficiency in our technique. Few references that have applied steganograpy and other related techniques.

The methodology of data hiding in least significant bits using hypothetical testing theory is being implemented in this paper (T. H. Thai *et al*., 2014). It exploits the heteroscedastic noise model which enhances the noise variance estimation and improves the detection performance. It also considers the clipping picture as criteria for hiding the data by analyzing overexposed and underexposed pixels which are statistically modelled and taken into account for pixel embedding. Generalized strategy of adaptive embedding and Prediction Error Expansion (PEE) is indulged in this paper (X. Gui *et al*., 2014). Complexity level and prediction values are computed and data is embedded in partition levels and the data size to be embedded at each level is selectively chosen for best performance. This results in high capacity redundancy with limited distortion.

A modern steganography method is used to perform anonymous communication by hiding the data bits in the sound container. The data is directly attached to the sound pixel and Fourier transform is applied on the processed signal. Masking phenomenon is being used and data is hidden in high frequency bands which improves the efficiency of concealing the information (G. Koziel., 2014).

Novel scheme of reversible data hiding which results in lossless compression of the encrypted data strategically reports to be quite feasible. Stream cipher has been used to mask the contents. The data hider compresses a part of data into the image using LDPC code. By exploiting both compressed data and additional information, the receiver can recover the original image without any error. Due to minimal changes in the encrypted text, it provides satisfactory results (X. Zhang *et al*., 2014).

The concept of novel blocks data hiding algorithm which improves the efficiency of JPEG steganography creates more impact on the standards of security. Matrix embedding method uses hamming parity check matrix and matrix multiplication whose computation complexity is high and only with one embedding change Matrix embedding (ME) cannot change the distortion level in JPEG steganography. Block data hiding (BDH) allows block of data to be hidden by changing two bits at the max. In addition to data hiding, data has been encrypted by a cellular based automaton. A non-repeating key stream is used and bitwise XOR has been applied in encryption process to maintain the speed and security (T.D. Nguyen *et al*., 2014).

This paper proposes a technique in which the image is encrypted using the hill cipher technique and it is embedded into the cover image using the least significant bit substitution technique and various scanning patterns like horizontal and vertical raster scan, horizontal and vertical snake and z scan (B. Karthikeyan *et al*., 2012). The improved steganography technique using LSB uses a raster scan along with a random key. This technique is suitable for embedding a large plain text to the cover image. Here the quality of the stego image is refined by applying the Optimal Pixel Adjustment Process (OPAP) (Amirtharajan *et al*., 2010; B. Karthikeyan *et al*., 2013).

In this paper, the message to be sent is encrypted modified blowfish algorithm and then embedded into

cover image (G. Manikandan *et al*., 2012; G.Manikandan *et al*., 2013). The resulting stego image is reduced using discrete wavelet transform and sent to the recipient. On the recipient side the reverse process is applied to get back the original message. A chaotic algorithm on steganography using discrete wavelet transformation helps to enhance the security of data (M. Ghebleh *et al*., 2014). This improves the robustness of the algorithm. Sweden's lifting scheme has been used for integer to integer transformation. This enhances the efficiency of the technique and provides flexibility.

In consideration of more secured data to be transmitted, Discrete Cosine Transforms (DCT) plays a major role and testifies the quality of the image based on different embedding positions. And the theoretical analysis proves that embedding the data in the low frequency part and image selection with rich pixel value improves the steganography performance (J.M. Zhou *et al*., 2013). Embedding based on statistical distribution alternating current DCT is carried out in this paper. A powerful blind detector is then constructed with proposed one dimensional feature. It also helps in finding out additive noise in the steganography process with low embedding rate. The proposed feature also identifies JPEG compression including stego image analyses (X. Li *et al*., 2014).

The scheme of integrating near field communication (NFC) and graphical password which assists in achieving secured and access control system. This is preceded using integration of steganography graphical password scheme into NFC which is enabled in Smartphone to transcend digital keys or tokens. The results depict the weight of security due to the behavioural intension to use the near field communication (S. N. Cheong *et al*., 2014). The methodology of imprinting audio files using Hermite transform (HT) with hidden messages approaches a new way of data hiding. The use of this technique enhances the efficiency in the algorithm. Performance is assessed based correlation and peak signal to noise ratio (S. L. Gomez-Coronel *et al*., 2014).

The idea of fusing blind source separation (BSS) technique and Maximum A Posterior (MAP) estimator introduces a new strategy of embedding technique. The inclusion of this method on minimum range of sources reduces the computational cost. This combination confirms the efficiency of the algorithm through required experiments (H. Modaghegh *et al*., 2014). Increasing the embedding capacity by implementing state-of-art schemes such as edge adaptive (EA) and highly undetectable stego. The trade-off between detect ability and embedding rate is calculated and higher the embedding rate, higher is the chance of detect ability. The classical steganography aims on providing high peak signal to noise ratio than undetectability. The results are analyzed and compared accordingly to provide better results (M. Afrakhteh *et al*., 2014).

Steganography based on discrete Gould transform, a new way of embedding technique. The Gould transform represents the difference in the neighbouring pixel of the image. This results in fragile steganography technique with high capacity. Any manipulation in the data results in destroying the data, hence helpful in authentication and security purpose (E. E. Varsaki *et al*., 2013).

This paper proposes a method in which mod 3 operation is performed on the secret image .Its observed that the result of mod 3 operations is 0, 1 or 2. The bytes of the original image is placed in any one of these data field (0, 1 or 3) based on the result of the mod 3 operation. These three data felid are then appended one after the other into the cover image. Here for the security purpose a pass-key is used which also serve as a delimiter between the layers. Enciphered text can also be included as one of the layers of the cover image. The reverse process is applied at receiver side to get back the original image and text (B. Elangovan *et al*., 2013).

RESULTS AND DISCUSSIONS

To implement the steganography technique, an image of random size is chosen and then converted to gray scale. The pixels are then converted to binary value so that the data could be embedded into it. The secret message from the sender is read in a file format and is being transformed using integer wavelet transformation.

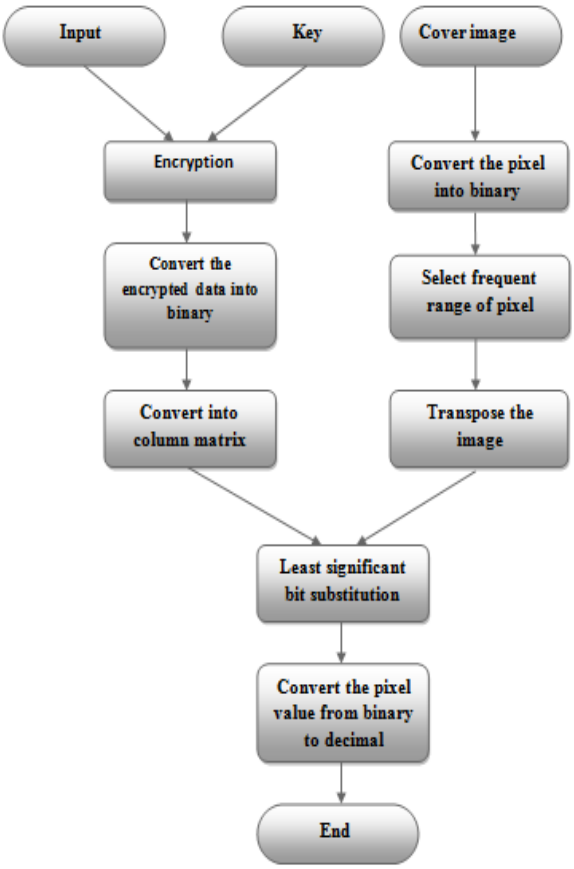

Figure-1. Steps involved in embedding the secret data into the image.

ALGORITHM

The input given to the system are cover image and confidential data which gets processed accordingly and produces the stego image as the output and has to be decrypted to extract the data.

Step-1: Read the secret message or the data in the file format.
Step-2: Convert the text into its corresponding ASCII value.
Step-3: Apply integer wavelet transformation to the ASCII value.
Step-4: To reduce complexity of negative numbers, subtract the transformed value from a large positive integer.
Step-5: Convert the decimal to binary representation.
Step-6: Reshape the contents into a single dimensional array.
Step-7: Get the cover image from the sender.
Step-8: Convert the pixel value into binary.
Step-9: Choose the pixels of certain range based on certain criteria.
Step-10: Binary data is embedded into the image using least significant bit substitution.
Step-11: Compute the mse value.
Step-12: IWT calculations applied on images of different types of text

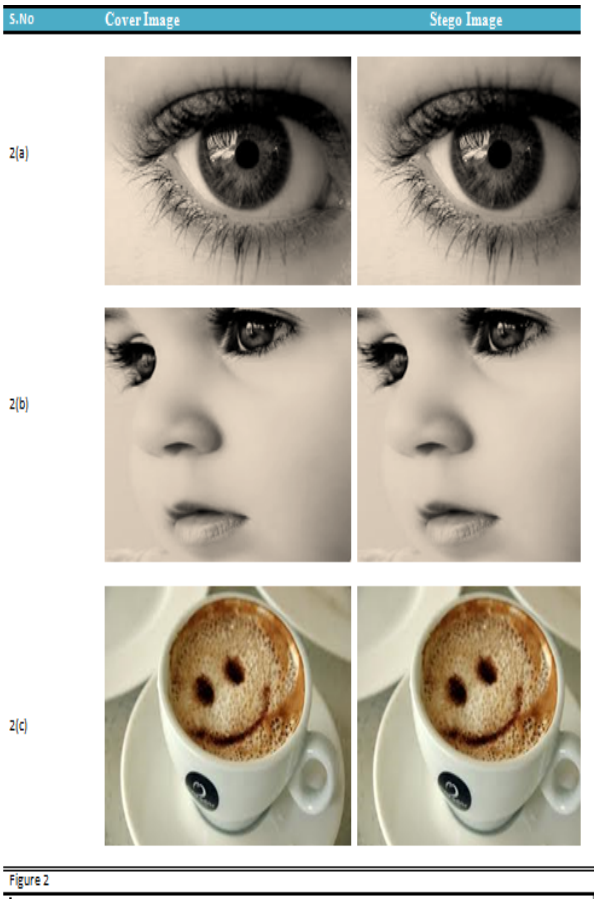

Figure-2. Cover image and corresponding stego images.

Table-1. Computation of MSE values for different sample images.

Image	image size	Text	text size	MSE
bab1.jpg	239X211X3	imp.txt	1X80	4.86E-04
bab1.jpg	239X211X3	save.txt	1X68	4.50E-04
eye.jpg	194X259X3	imp.txt	1X80	5.05E-04
eye.jpg	194X259X3	save.txt	1X68	4.32E-04
friends.jpg	183X275X3	imp.txt	1X80	5.14E-04
friends.jpg	183X275X3	save.txt	1X68	4.69E-04
lena.jpg	256X256X3	imp.txt	1X80	3.85E-04
lena.jpg	256X256X3	save.txt	1X68	3.82E-04

Statistically Mean Square Error estimates the difference between experimentally estimated value and the true value, which signifies the loss in the quality or quantity of the work done. Here Mean square error [20, 21] is calculated to know the amount of deviation in pixel value after embedding the transformed data bits into it. The estimation of MSE (as shown in Table-1) showcases the quality change in the stego image, which has to be maintained in order to benefit the methodology.
MSE is calculated using the following formula

$$MSE = \frac{1}{mn\sum_{i=1}^{m}\sum_{j=1}^{n}(x(i,j) - y(i,j))^2}$$

CONCLUSIONS

This paper proposes combination of Integer Wavelet Transformation and Lest Significant Bit substitution which intensifies complexity of the cipher text (as shown in Figure-1), making it difficult for cryptanalysis, which then masquerades the secret data into the image such that there is only a meager difference between the original cover image and the stego image(as shown in Figure-3). The complexity level increases by induction of random pixel selection which augments the security of data. This indiscriminate approach varies according to the diffusion of various intensities in the image. This procedure enables us to achieve ameliorated security than the other traditional methods.

REFERENCES

Afrakhteh M., Moon I and Lee J.A. 2014. Double phase modular steganography with the help of error images. Multimed. Tools Appl. pp. 1-15.

Ajit Singh and Swati Malik. 2013. Securing Data by Using Cryptography with Steganography. Int. J. Adv. Res. Comp. Sci. Soft. Engg. 3: 404-409.

Amirtharajan R and Rayappan J.B.B. 2012. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: a comparative study on PI stego. Res. J. Inform. Technol. 4, 4:124-139.

Amirtharajan R., Adharsh D., Vignesh V and John Bosco Balaguru R. 2010. PVD Blend with Pixel Indicator - OPAP Composite for High Fidelity Steganography. Int. J. Comput. Appl. 7, 9: 31-37.

Chan C.K. and Cheng L.M. 2004. Hiding Data in Images by Simple LSB Substitution, Pattern Recognition, 37:469-474.

Chang C.C., Chen T.S and Chung L.Z. 2002. A steganographic method based upon JPEG and quantization table modification. Inform. Sci. 141: 123-138.

Cheong S.N., Ling H.C and Teh P.L. 2014. Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smart phone access control system. Expert Systems with Appl., 41, 7:3561–3568.

De Vos A., Burignat S and Thomsen M.K. 2012. Reversible implementation of a discrete integer linear transformation. J. Multiple-Valued Logic Soft Computing. 18, 1: 25-35.

Elangovan B. and Mohana S. 2013a. An efficient steganographic method by using Image Fragments With High Security. Res. J. Inf. Technol. 5: 456-461.

Elangovan B., Rajesh K and Venkateswari P. 2013b. An efficient method for high secured image steganography using image segments. Int. J. Applied Sci. Eng. 12: 1395-1403.

Ghebleh M. and Kanso A. 2014. A robust chaotic algorithm for digital image Steganography. Communications in Nonlinear Science and Numerical Simulation, 19, 6:1898-1907.

Gomez-Coronel S.L., Escalante-Ramirez B., Acevedo-Mosqueda M.A and Mosqueda M.E.A. 2014. Steganography in audio files by Hermite Transform. Applied Mathematics Inf. Sci. 8, 3: 959-966.

Gui X., Li X and Yang B. 2014. A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding. Signal Process. 98: 70-380.

Karthikeyan B., Chakravarthy J and Ramasubramanian S. 2012. Amalgamation of scanning paths and modified hill cipher for secure steganography. Australian J. Basic Applied Sci. 6, 7: 55-61.

Karthikeyan B., Ramakrishnan S., Vaithiyanathan V., Sruti S and Gomathymeenakshi M. 2013. An improved steganographic technique using LSB replacement on a scanned path image. Int. J. Net. Security. 15, 1: 314-318.

Koziel G. 2014. Simplified steganographic algorithm based on Fourier transform, Adv. Sci. Letters. 20, 2: 505-509.

Li X., Zhang T., Zhang Y., Li W and Li K. 2014. A novel blind detector for additive noise steganography in JPEG decompressed images. Multimed. Tools Appl. 68, 3: 1051-1068.

Manikandan G., Kamarasan M and Sairam N. 2013. A new approach for secure data transfer based on wavelet transform, Int. J. Net. Security. 15, 2: 106-112.

Manikandan G., Kamarasan M., Rajendiran P and Manikandan R. 2011. A hybrid approach for security enhancement by modified crypto-stegno scheme. European J. Scientific Res. 60, 2: 224-230.

Manikandan G., Rajendiran P., Chakarapani K., Krishnan G and Sundarganesh G. 2012. A modified crypto scheme for enhancing data security. J. Theoretical Applied Info. Technol. 35, 2: 149-154.

Mehboob B. and Faruqui R.A. 2008. A stegnography implementation. IEEE- International Symposium on Biometrics and Security Technologies.

Modaghegh H and Seyedin S.A. 2014. A new fast and efficient active steganalysis based on combined geometrical blind source separation. Multimed. Tools Appl.

Mukherjee S., Deb M. Agarwal P.K and Roy A. 2012. A new approach to stegnography. 2nd International Conference on Computer Science and Information Technology.

Nguyen T.D., Arch-int S and Arch-int N. 2014. A novel secure block data-hiding algorithm using cellular automata to enhance the performance of JPEG steganography. Multimed. Tools Appl. 1-22.

Padmaa M. and Venkataramani Y. 2014. Encrypted Secret Blend with Image Steganography for Enhanced Imperceptibility and Capacity. Res. J. Inf. Technol. 6: 342-355.

Po-Yueh Chen and Hung-Ju Lin, 2006. A DWT based approach for image steganography. Int. J. Applied Sci. Eng. 4, 3: 275-290.

Ramalingam B., Amirtharajan R. and Rayappan J.B.B. 2014. Stego on FPGA: An IWT Approach. Sci. World J., 10.1155/2014/192512.

Shilpa Sunil Wankade and prof. Ramesh V Shahabade. 2013. Secured data transmission through steganography and RSA cryptography for VOIP. International Conference on Electrical Engineering and Computer Science.

Tao Zhang. Wenxiang Li. Yan Zhang. Ergong Zheng and Xijian Ping. 2010. Steganalysis of LSB matching based on statistical modeling of pixel difference distributions. Info. Sci. 180: 4685-4694.

Thai T.H., Retraint F. and Cogranne R. 2014. Statistical detection of data hidden in least significant bits of clipped images. Signal Process. 98: 263-274.

Thanikaiselvan V., Arulmozhivarman P., Amirtharajan R and Rayappan J.B. 2011. Wavelet pave the trio travel for a secret mission - A stego vision. 4th International Conference on Global Trends in Information Systems and Software Applications, Vellore, TN, India, December 9-11, 2011 proceedings, part II, pp. 212-221.

Varsaki E.E., Fotopoulos V and Skodras A.N. 2013. A discrete Gould transforms data hiding scheme. Mathematical Methods in the Applied Sci. 37, 2: 283-288.

Yang C.H. 2008. Inverted pattern approach to improve image quality of information hiding by LSB substitution. Pattern Recognition. 41: 2674-2683.

Yang L., He X., Zhang G., Qing L and Che T. 2013. A low complexity block-based adaptive lossless image compression. Optik. 124, 24: 6545-6552.

Young-Ran Park., Hyun-Ho Kang., Sang-Uk Shin and Ki-Ryong Kwon. 2005. An image steganography using pixel characteristics. Springer-Verlag. 3802, 581-588.

Zhang X., Qian Z., Feng G and Ren Y. 2014. Efficient reversible data hiding in encrypted images. Journal of Visual Communication and Image Representation. 25, 2: 322-328.

Zhou J.M., Pan Y and Yang R.E. 2014. DCT-based digital image steganography. 4th International Conference on Frontiers of Manufacturing and Design Science, September 10-12, 2013, Hong Kong, China, part 4. pp. 1986-1990.