Journal of Engineering and Applied Sciences 12 (Special Issue 10): 8875-8881, 2017
ISSN: 1816-949X

High Security Steganography Model Based on DWT, DCT and RSA

Ali Kadhim Bermani
College of Information Technology, University of Babylon, Hillah, Iraq

Abstract: The steganography is the science of concealing secret information in media files (i.e., image, text, audio, etc.), so that, such information is not noticeable by the eavesdropper. There are many techniques are used to hide secret information to achieve high quality of stego image and high embedding capacity. Also, many challenges in steganography including the attempts to reveal these secret information that has been hidden. A plenty of researches have tried to develop a lot of techniques and algorithms to find solutions to this problem. This study proposed high security model for hiding image (secret image) in another image (cover image) where more than one algorithm has been utilized such as: Discrete Wavelet Transform (DWT) algorithm and applied DCT algorithm to compression the secret image and provide more space for hiding secret image and applied RSA algorithm to encryption and provide more secure. Certain quality metrics such as Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) also Compression Ratio (CR) have been used to calculate the quality of the this model. The proposed model is implemented using visual basic 6 programming language.

Key words: Steganography, stego image, Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Rivest-Shamir-Adleman (RSA), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR)

INTRODUCTION

Steganography can literally be interpreted as "hidden writing". Information concealment is often associated with the inclusion of data in a form of digital media (Weiss, 2004). In 1499, the first use of the Steganography reform was by Ohannes Trithemius in his book "steganography" which was specialized in coding and grading and published in the same year (Lovepreet, 2014). The major intention of steganography is to conceal secret information in media, so that, only authorized persons can see it (Richard, 1998). Figure 1 shows fundamental process of steganography.

Types of steganography are can be divided according to the media used to hide secret information and it divided into the following.

Steganography based on text: This technique uses printed normal text to hide secret information. Historically, the method of concealing information in texts is considered an important method of concealment. Also, steganography based on text that utilizing media is not usually used, since, text files do not contain too much unnecessary data (have small amounts of redundant data) (Morkel *et al*., 2005).

Steganography based on audio: This technique uses audio file as cover file to hide secret information.

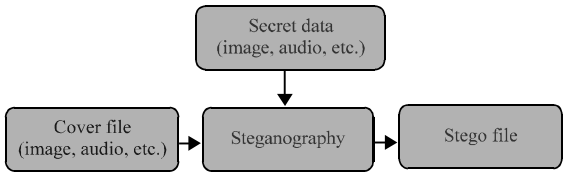

Fig. 1: Fundamental process of steganography

Steganography based on image: This technique uses images to hide the secret information. In addition to that hiding information in digital images is one of the most popular way for several reasons. Digital images contain a lot of extra bits that can be replaced with secret data without any difference between them and the original image. The increasing use of digital images in digital media and the internet, particularly social media. Furthermore, there are 2 types of Image steganography techniques: spatial domain technique implant secret information in the intensity of the pixels straightforwardly. Transform domain or frequency domain, images are first transformed and then the secret information is embedded in the image (Juneja and Sandhu, 2009; Ali and Kadhim, 2016).

Steganography based on protocol: This technique uses network control protocols used in network transmission to embedding information within messages (Ahsan and Kundur, 2002) (Fig. 2).

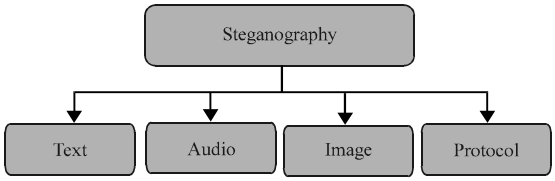

Fig. 2: Steganography types

Also, the types of steganography techniques can be divided according to the methods used to hide information and it divided into the following.

Substitution technique: The principle of this technique is to replace bits with the least significant bits of the cover file being replaced without modifying all the data in the cover file. This technique is one of the simplest ways to hide data but it is easy to detect and can be detected by simplest means of detection such as pressure, transfers, etc.

Transform domain technique: The principle of this technique is to make some transforms in the domains. The examples of this technique are: FFT, DWT and DCT they are used to hide information in transform coefficients of the cover images that make much more robust to attacks such as compression, filtering, etc.

Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information.

Statistical technique: The principle of this technique is to divide the cover file into blocks and hide certain bits of the concealed data in each block. We can simply encode the information throughout the change of different statistical features of the cover file.

Distortion technique: The principle of this technique is signal distortion to store Information. The encoder adds sequence of changes to the cover and the decoder checks for the various differences between the genuine cover and the indistinct cover to recover the secret message (Reddy and Raja, 2009; Arora *et al*., 2014). Figure 3 shows types of steganography techniques.

In the science of steganography, there are three fundamental aspects that must be taken under consideration to ensure the quality of the steganography system (Lin and Delp, 1999).

Capacity: This aspect refers to the sum of data that can be concealed in the cover file, the greater the quantity of data that can be hidden the better steganography system is.

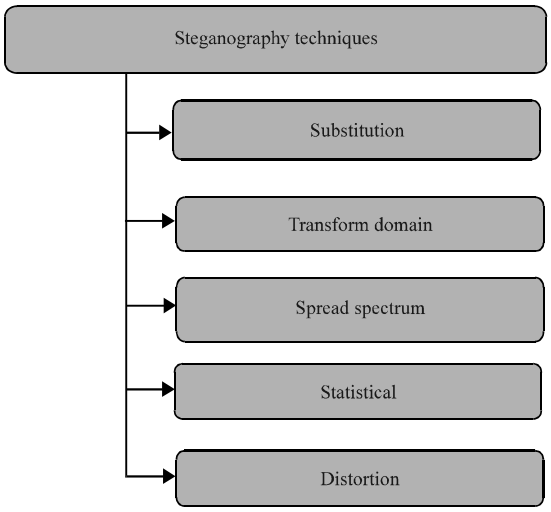

Fig. 3: Types of steganography techniques

Security: This aspect refers to the level of security in the transfer of confidential information, this depends on the level of difficulty of disclosure of confidential information by unauthorized persons to access secret information and the concealment of steganography system is of high quality if the access to the information is difficult.

Robustness: This aspect refers to the amount of modification the stego medium can withstand before an adversary can destroy hidden information (Al-Ataby and Al-Naima, 2008).

In this study, the proposed model is used to hide an image inside another image, taking under consideration the three aspects of the quality of the steganography system. A DCT algorithm has been applied to compress the secret image in order to allow a greater size of concealed data. Thus, the first aspect (capacity) has been used to hide data. In addition, the RSA algorithm has been used for encoding image which was applied to the secret image after the compression in order to achieve strength to the system where it is difficult to discover the secret image and know the details, thus, we achieved the second aspect of the efficiency of the model. Also, DWT algorithm were used on the cover image because DWT conversions increases the robustness of the steganography system of the eavesdropper. Therefore, this model has achieved all aspects to ensure the quality of the concealment steganography system.

Discrete wavelet transform: DWT algorithm is using to convert the data from spatial domain to frequency domain which the resulting wavelet coefficients are modified to hide the data. These the wavelet coefficients will

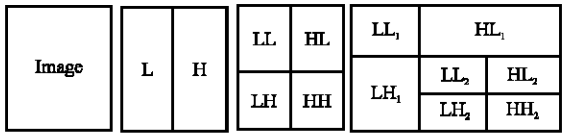

Fig. 4: Illustration of 2 level decomposition DWT of an image

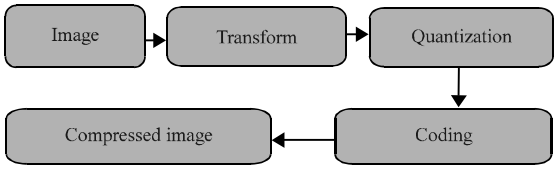

Fig. 5: Image compression model

separates to high and low frequency data on a pixel to pixel basis (Chen and Lin, 2006). In 1D-DWT that is a repeated filter bank algorithm the input data is converted with two filters, the first pass filter is the high pass filter and the second filter is the low pass filter, the result is a stacked version of the input while the high-frequency segment is captured by the first flap. In 2D-DWT, the first step is apply one dimensional transform to all rows in image. Then, repeat the same for all columns. The second step, the coefficients that result from a convolution in both directions. These steps result in four bands of coefficients namely the approximate band (LL), Horizontal band (HL), vertical band (LH) and the diagonal band (HH). In this study using the Haar wavelet transform is one of the most famous wavelet transform. The low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained ("LL, HL, LH and HH"). The approximation band (LL) consists of low frequency wavelet coefficients which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients which contain the edge details of the spatial domain image. The DWT technique describes the decomposition of the image in four non overlapping sub-bands with multi-resolution. This process can be iterated on one of the sub-band of first level DWT to get the further second level sub-bands for better results. Figure 4 illustration of 2 level decomposition DWT which were used in this study.

Discrete Cosine Transform (DCT): In digital images, the larger image size, the more accurate it becomes. So,we tried to have a large secret image size in order to accommodate a greater accuracy, however, the use of a large sized secret image may expose it to the intruders access. In order to overcome this problem we can simply use one of the compression algorithm. One of the basic ways to compress data (image, audio, video, etc.) is the Discrete Cosine Transform (DCT). It works on dividing the image into small blocks of pixels and transform from the spatial domain to values in the frequency domain. Figure 5 shows Image compression model.

In this study, we used DCT algorithm proposed by Kapoor and Patyal (2014) but here the researcher used 2DCT with compression factor of 4×4 because it provides a good compression ratio and the quality of the image that we obtained is good.

Therivest-Shamir-Adleman (RSA): In order to increase security in hidden information (image) and make that information incomprehensible to those who are trying to detect hidden information, it is therefore, desirable to encrypt those data. In this study, The Rivest-Shamir-Adleman (RSA) algorithm was used to encrypt confidential data before hiding it. Ron Rivest *et al*. developed RSA algorithm in 1977. RSA is a cryptosystem which is also known as public key cryptography. This type of cryptography uses two different keys: the first one is public key, so that, it shares with everyone and the second is private key that remains secret, both keys (public and private) are mathematically linked. In RSA algorithm, both the (public and private) keys can encrypt the data, so, the RSA algorithm is considered the most widely used as well as provides a way to ensure the confidentiality and integrity of data. This algorithm will make the information to be transmitted into an unintelligible form by encryption, so that, only authorized persons can correctly recover the information. The cryptographic algorithm used in this study is the RSA algorithm presented by Chepuri (2017). It's modified for color image encryption. The image encryption and decryption approaches are highly securable and with less computational time and the result of this approach is an efficient cryptosystem for image encryption and it is suitable for secured transmission of images over the internet. Figure 6 shows block diagram of encryption and decryption RSA algorithm proposed by Chepuri (2017). The purpose of using the RSA algorithm in this study is to increase safety in the proposed steganography model, so that in the case of the steganalysis and detect of hidden data will not detect the original secret image that was hidden because it was encrypted.

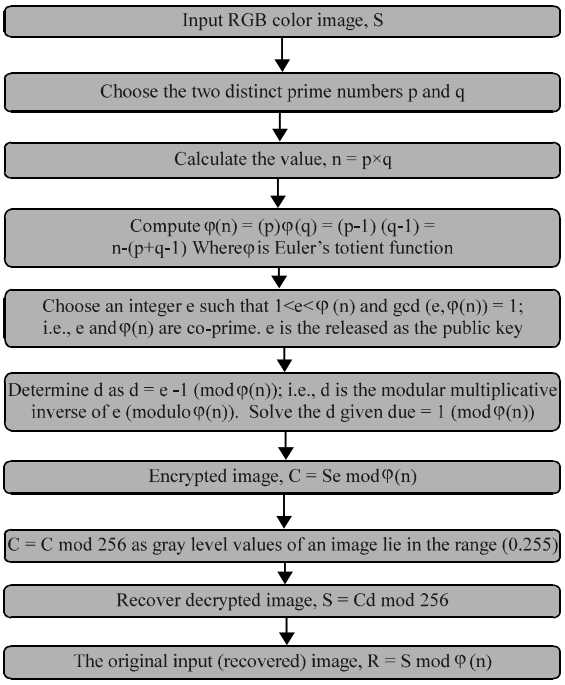

Fig. 6: Block diagram of encryption and decryption RSA algorithm proposed by Chepuri (2017)

MATERIALS AND METHODS

The proposed model has two major stages:

Embedding stage: This stage refers to the hiding of the secret image inside the cover image. It includes the processing of the secret image which contains the compression of the secret image by the DCT algorithm after that the image is encoded by the RSA algorithm and resulting image is the secret image that we want to hide. the main reason for the compression of the secret image is to provide a greater opportunity to use a large-sized image to hide and the main reason for encryption the image is the difficult to detect the secret image or even if revealed its difficulty to decrypt and thus keep our confidential information. Also within this stage the DWT algorithm is used with the cover image and embedding with secret image by an embedding process, then the resulting image will be the stego image. The following are the steps to build embedding stage in the proposed model.

Step 1; input the original image (cover image): In this step, we conducted the two levels of DWT on the cover image. This in effect will make the formation of four bands (LL_1, HL_1, LH_1 and HH_1). And then the DWT transform is conducted for the second time on the HH band to gain the subsequent coarser scale of wavelet

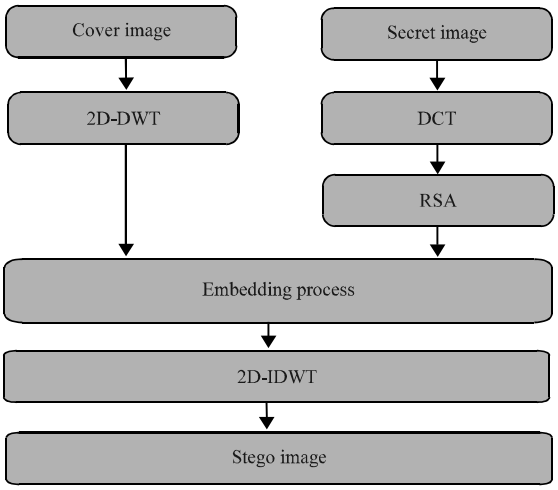

Fig. 7: Block diagram of embedding stage of proposed steganography model

coefficients leading to another level of sub-domains in (HH_1) band as (LL_2, HL_2, LH_2 and HH_2). There we will embed the secret data in (LL_2) band due to the concealment of the approximate domain which facilitates the receiver's extraction of the secret data.

Step 2: Input the secret image and then uses DCT algorithm that uses 2DCT with compression factor of 4×4 to guarantee that the ratio between the compression ratio and image quality is equivalent.

Step 3: Apply RSA algorithm on the secret image (that produced from step 2). The purpose of apply this algorithm is to increase the safety in the proposed model.

Step 4: Embedding process, in this step the starting point begins from the upper left corner of the LL_2 level band and to replace the 4 LSB of the LL_2 band coefficient by 4 MSB of the secret image pixel, repeat this step for N times (where N×N is the size of the secret image), thus we gain the embedded secret.

Step 5: Apply 2D-IDWT to retranslate the frequency domain information to the spatial domain. This will lead to get an image (stego image) similar to the original image (cover image). When the stego image is transferred over the network, the main information must be sent to the receiver because without the prior knowledge of main information the secret image cannot be extracted. The main information is the random combination of the size of the secret image (N×N), the name of the band where the secret is embedded (LL2) and the number of MSB bits of the secret embedded (4 MSB). Figure 7 shows the block diagram of secret image embedding procedure of steganography.

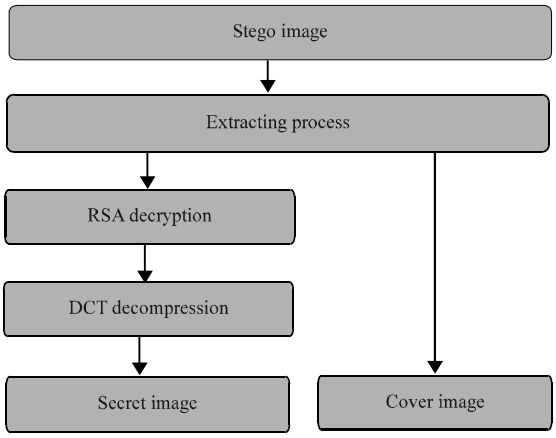

Fig. 8: Block diagram of extracting stage of proposed

Extracting stage: This is the stage of extracting the secret image from the stego image. This stage contains some simple steps that are just reverse to the embedding process. It simply employs the Haar DWT operations and the corresponding extraction of the MSB of the secret. The following are the steps to build extracting stage in the proposed model.

Step 1; The input is stego image: The receiver has the prior knowledge of the location of the secret as it is provided in the form of main information. The stego image is transformed from the spatial domain to the frequency domain by conducting the 2DWT procedures over it. Finishing this step, the receiver gets the LL_2 band wherein it includes the secret image's bits.

Step 2; Extracting process: In this step, the starting point begins from the upper left corner of the (LL_2) band, pull out the 4 LSB into a new matrix vector. After iterating this step N times (where N is the size of the secret image as provided by the sender included in the main information), we get the original image and the secret image in an N×N matrix.

Step 3: Apply the decryption steps of the RSA algorithm on the secret image generated from the previous step.

Step 4: Apply the decompression steps of the DCT algorithm on the image generated from the previous step. This will lead to get an image (secret image) similar to the original image (secret image). Figure 8 shows block diagram of secret image extracting procedure of steganography.

Performance quality measurements: There are some measures to measure the quality of the stego image and the secret data extracted from them, as well as some measures for measuring the compressed image and compression ratios. These metrics gives the comparison ratio between the original image and stego image as well as provide us a comparison of images before and after comparison. The metrics used in this study are as follows:

Mean Square Error (MSE): MSE is one of the most important quality measures and most commonly used. It's the measure of average of the squares for the difference between the intensities of the stego image and the cover image (Verma *et al*., 2013). The large value of MSE means that image is poor quality. It's represented as:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (S_{i,j} - V_{i,j})^2$$

Where:
$S_{i,j}$ = The cover image
$V_{i,j}$ = The stego image

Peak Signal to Noise Ratio (PSNR): PSNR is one of the most famous quality measures and used to distinguish between the cover image and the stego image. It's defines between the maximum possible power of a signal and the power of corrupting noise. The large value of Peak Signal to Noise Ratio (PSNR) means that image is of good quality. It is formulated as:

$$PSNR = 10 \frac{\log_{10} (255)^2}{\frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (S_{i,j} - V_{i,j})}$$

Compression ratio: To calculate compression ratio:

$$CR = \frac{\text{Original size-Compressed size}}{\text{Original size}} \times 100$$

RESULTS AND DISCUSSION

To test the efficiency of this study, a number of experiments were studied as shown in the following tables: Table 1 shows the original secret images and the size of the original and compression images and compression ratio. While Table 2 shows the cover images, original secret images, stego images and PSNR, MSE which used to evaluate this model.

Table 1: The secret images used and the size of the original and compression image by 2DCT in byte

Secret image	Size of the secret image (K)	Compressed size (K)	CR
	31.0	10.2	67.09
	22.6	7.73	65.79
	35.2	12.2	65.34
	35.9	11.1	69.08

Table 2: The cover images, original secret images, stego images and PSNR, MSE which used to evaluate this model

Cover image 1024×768	Original secret image 256×256	Stego image	PSNR	MSE
			86.68	0.524
			78.88	0.565
			74.67	0.586
			72.49	0.621

CONCLUSION

In this study, a model was proposed model to hide image in other image using some algorithms including DWT, DCT and RSA. This model is divided into two stages. The first is the embedding stage. The second is the extraction stage. In this proposed model, the main aspects of the success of the steganography model were taken into consideration (capacity, security, robustness). In this model, some measures were used to test the strength of the model such as PNSR, MSE and CR. The extracted secret image is similar to the original confidential image. And we can say that this model provided the following:

- This model provide more secure system using RSA with steganography
- Using the DCT algorithm provide more space for hiding secret image
- The second level DWT for steganography provide the robustness

REFERENCES

Ahsan, K. and D. Kundur, 2002. Practical data hiding in TCP/IP. Proceedings of the Workshop on Multimedia Security at ACM Multimedia Vol. 2, December 6-9, 2002, ACM, Juan-les-Pins, France, pp: 1-8.

Al-Ataby, A. and F. Al-Naima, 2008. A modified high capacity image steganography technique based on wavelet transform. Intl. Arab J. Inf. Technol., 7: 358-364.

Ali, B.K.S.M.H. and A.B. Kadhim, 2016. An efficient steganography model using video compression and image steganography. J. Babylon Univ. Pure Appl. Sci., 24: 1145-1154.

Arora, P., A. Agarwal and Jyoti, 2014. A steganographic method based on integer wavelet transform and genatic algorithm. Intl. J. Eng. Res. Appl., 4: 34-40.

Chen, P.Y. and H.J. Lin, 2006. A DWT based approach for image steganography. Int. J. Applied Sci. Eng., 4: 275-290.

Chepuri, S., 2017. An RGB image encryption using RSA algorithm. Intl. J. Curr. Trends Eng. Res., 3: 1-7.

Juneja, M. and P.S. Sandhu, 2009. Designing of robust image steganography technique based on LSB insertion and encryption. Proceedings of the International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom'09), October 27-28, 2009, IEEE, Kottayam, Kerala, India, ISBN:978-1-4244-5104-3, pp: 302-305.

Kapoor, P. and S. Patyal, 2014. DCT image compression for color images. Intl. J. Recent Innovation Trends Comput. Commun., 2: 3247-3252.

Lin, T. and J. Delp, 1999. A review of data hiding in digital images. Image Capture Syst. Conf., PICS, 52: 274-278.

Lovepreet, K., 2014. Steganography process a review. Intl. J. Innovative Res. Comput. Commun. Eng., 2: 4857-4861.

Morkel, T., J.H.P. Eloff and M.S. Olivier, 2005. An overview of image steganography. Proceedings of the 5th Annual Information Security South Africa Conference, June 29-June 1, Sandton, South Africa, pp: 1-12.

Reddy, H.M. and K.B. Raja, 2009. High capacity and security steganography using discrete wavelet transform. Intl. J. Comput. Sci. Secur., 3: 462-472.

Richard, P., 1998. An analysis of steganographic techniques. MSc Thesis, Faculty of Automatics, Department of Computer Science and Software Engineering, The University of Timisoara, ?Timisoara, Romania.

Verma, A., R. Nolkha, A. Singh and G. Jaiswal, 2013. Implementation of image steganography using 2-level DWT technique. Intl. J. Comput. Sci. Bus. Inf., 1: 1-14.

Weiss, M., 2004. Principles of steganography. Introduction Cryptography, 1: 1-3.