Research journal of Applied Sciences, Engineering and Technology 4(17): 3031-3039, 2012
ISSN: 2040-7467

Submitted: January 10, 2012 Accepted: February 09, 2012 Published: September 01, 2012

Security Evaluation of DWT Based Watermarking Schemes and its Improvement Using RS Coding

Amir reza Fazli, Mohammad Eghbali Asli and Ghazale Sarbisheie
Department of Computer Engineering, Science, Sadjad Institute of Higher Education, Mashhad, Iran

Abstract: In this study, information theory is used to provide both theoretical and practical analysis of security offered by watermarking and data hiding techniques based on wavelet transform. In this context, security level is defined as the equivocation of the secret parameters. On the theoretical side, the measure of security is estimated by means of information theory tools for all possible attacks. On the practical side, simulations assess the security levels derived in the theoretical part of paper to reveal the fundamental limits and bounds on security and show the trade off between security and other properties, such as robustness and imperceptibility. Also, the error correcting codes is used to decline effects of these limits. Experimental works indicate that the error correcting codes, such as Reed-Solomon code can be greatly effective for increasing the security of many watermarking schemes.

Keywords: Equivocation, error correcting codes, information leakage, watermarking security, wavelet transform

INTRODUCTION

With the rapid development of communication networks and computers, multimedia distribution via the internet has become very popular. Because of its nature, it has become easier and easier to access and redistribute digital multimedia data. Hence, the enforcement of multimedia copy right protection has become a very important issue.

This study considers security of digital watermarking as an effective instrument against piracy. One of the first attempts to provide a modern terminology of watermarking security and steganography presented by Simmons (1984) is prisoner's problem that Alice and Bob in a jail plane to escape together. All communications between them are monitored by Wendy, a warden. Therefore, they must hide the message in other cover-objects to obtain the stego-object. Then, the stego-object is sent through the public channel. Wendy can check all the messages between Bob and Alice with two options, passive and active. The passive way is to check the message in order to determine wether it contains a hidden message and then to conduct a proper action. On the other hand, the active way is to modify message though Wendy may not perceive any trace of a hidden message. In this study, we focus on the passive warden. Papers presenting a complete analysis of watermarking security are extremely rare. The authors are only aware of the recent works sketching a general framework for security analysis (Barni *et al*., 2003; Cayre *et al*., 2005) where, the goal is to adapt Shannon's definition of cryptography security to watermarking. Fisher's information matrix is used to measure the leakage of information by means of attacker's observations (Cayre and Bass, 2008). The main idea is that information about the secret keys leaks from the observations, for instance, watermarked pieces of content, available for opponent. Also, the security of spread spectrum watermarking has been addressed in Bahat *et al*. (2010). As a famous work on watermarking security, Comesana *et al*. (2006) resort to the Shannon's equivocation instead of the Fisher information for performing theoretical analysis.

Digital watermarking studies have always been driven by the improvement of robustness. Robust watermarking is defined as a communication channel multiplexed into original content (Kalker, 2001). On the contrary, security has received little attention in the watermarking community. The first difficulty is that security and robustness are neighbouring concepts, which are hardly perceived as different. Indeed, there are a number of desirable characteristics that a watermarking technique should exhibit. We use the general definition proposed in Moulin (2001):

Corresponding Author: Amir reza Fazli, Department of Computer Engineering, Science, Sadjad Institute of Higher Education, Mashhad, Iran, Tel.: +98912-140-9115

- **Security:** A watermark should be secret and must be undetectable by an unauthorized user in general. This requirement is regarded as security and watermark is usually achieved by the use of privet secret keys.
- **Robustness:** The digital watermark is still present in the image after attack and can be detected by the watermark detector. Possible attacks include linear or nonlinear filtering, resizing and image compression.
- **Imperceptibility:** One of the main requirements for watermarking is the perceptual transparency. The digital watermark should not be noticeable to the viewer. The data embedding process should not introduce any perceptible artifacts into original image and not degrade the perceived quality of the image.

Moreover, Barni *et al*. (2003) proposed a watermarking technique by embedding a watermark in the discrete cosine transform (DCT) domain using the concept of spread spectrum communication which is robust and secure against different types of attacks.

Kutter *et al*. (2001) presented the spread spectrum image watermarking technique in the discrete wavelet transform (DWT) domain. They embed a watermark with a constant weighting factor into perceptually significant coefficients in the high frequency sub bands in order to preserve imperceptibility. However, it is not robust to common signal processing attacks. Consequently, a digital watermarking technique should satisfy all important watermarking properties.

In this study, we have presented a complete analysis of a typical watermarking system by considering information theory and Shannon's measure of perfect secrecy. We have derived equivocation, as a measure of security, for different attack scenarios in a watermarking system. In order to improve security in watermarking systems, we have used error correcting codes and we have shown that these codes can improve security level and decrease bit error rate of watermark extraction.

METHODOLOGY

Notation:

Let us first list some notational conventions used in this study.

X is a finite set of vectors representing a collocation of original image.

Y is a finite set of vectors representing a collocation of watermarked image.

Nw is the size of watermark vector.

Ns is the size of appropriate coefficients vector for watermark embedding.

We also need to define what we consider a secret key in this work. We use the general formulation proposed in Cheng Liu *et al*. (2006): The secret key is a list of Nw integers $K=\{k(1),\ldots\ldots, k(Nw)\}$ with $\leq k(i) \leq Ns$, also we assume that the secret key is chosen independent of the watermark. Moreover, in order to have more secrecy, we suppose that the probability distribution for K is uniform.

Watermarking based on DWT: The basic idea of DWT for a two dimensional image is described as follows. An image is first decomposed into four parts of high, middle and low frequencies (i.e., LL1, LH1, HL1 and HH1 sub bands) by fatally sub sampling horizontal and vertical channels using sub band filters. The sub bands labelled LL1, LH1, HL1 and HH1 represent the finest scale wavelet coefficients. To obtain the next coarser scaled wavelet coefficients, the sub band LL1 is further decomposed and critically sub sampled. This process is repeated several times, which is determined by the application at hand. Moreover, from these DWT coefficients, the original image can be reconstructed. This reconstruction process is called the inverse DWT (IDWT). The DWT and IDWT for an image can be similarly defined by implementing the DWT and IDWT on each dimensions of image separately. In this study, we use the watermarking QSWT technique for watermarking proposed in Wang (2004). This method is based on the wavelet transform. Unlike most previous works, which used a random number of sequences of bits as a watermark, this method embeds a watermark with visual recognizable patterns, such as binary or gray or colour images by modifying the frequency part of the images. In this method, an original image is decomposed into wavelet coefficient, then, Qualified Significant Wavelet Tree (QSWT) is used to select the locations where the pixels of watermark is to be embedded. This algorithm uses a threshold value T, to determine appropriate wavelet coefficients for data embedding. Since this threshold directly determines the number of selected coefficient, it has an important role in security measurements.

Shannon's methodology: The methodology presented in this section is clearly inspired by the cryptanalysis. It has already been presented in Barni *et al*. (2003). The methodology that Shannon exposed for studying the security of encryption schemes is here transposed to watermarking. The watermarker has randomly picked up a secret key and used it to watermark several pieces of content. The opponent observes these pieces of watermarked content. The watermarking technique is secure if and only if no information about the secret keys leaks from the observations. The bigger the information leakage is, the smaller the security level of the watermarking technique will be.

Watermarking security: If a watermarking scheme does not provide perfect secrecy, then one would like to measure the information leakage on the secret key. For this purpose, we present several tools from information theory, which will later be helpful to analyse the security of watermarking system.

Shannon's measure: In order to analyse a wavelet based watermarking from an information theoretic point of view, we make a clear definition of Shannon's theory regarding perfect secrecy. An encryption scheme has perfect secrecy iff I (K |O) = 0

This means that in a perfect covering scheme, the observation do not reveal any information about the secret key K. In the case where the secret key is a discrete variable, the entropy H (K) measures the uncertainty of the opponent on the true value of K. When the opponent makes observation O, his uncertainty is evaluated through conditional entropy, which Shannon named equivocation:

$$H(K|O) = H(K) - I(K|O) \quad (1)$$

The information leakage is measured by the mutual information between observation and security key.

Possible attacks: Watermarking security was first considered from the point of view of security level assessment. In this section, we define a classification of attacks according to type of information which the opponent has access to:

- A Known Message Attack (KMA) that occurs when an attacker has access to several pair of watermarked contents and corresponding hidden messages.
- A Known Original Attack (KOA) that occurs when an attacker has access to several pair of watermarked contents and corresponding original versions.
- A Watermarked Only Attack (WOA) that occurs when an attacker has access to several pair of watermarked contents.

Information theory based analysis: In this section, we present an estimation of the information leakage and equivocation in watermarking systems under different attacks via information theory tools.

security analysis for KMA scenario: In this case, the opponent only has access to watermarked vector Y and the associate message (Y, M).

Therefore, the information leakage is:

$$I(Y; K|W) = H(K|W) - H(K|W, Y) \quad (2)$$

Also equivocation is denoted by $H(K|W, Y)$
We have:

$$H(K|W, Y) = H(K, W, Y) - H(W, Y)$$

$$= H(K, W) + H(Y|K, W) \quad (3)$$

It is obvious that: $H(Y|K, W) = 0$

Also, we know that, the watermark and secret key are independent. Hence we have:

$$H(K|W) = H(K); \text{ and } H(K, W) = H(K) + H(W).$$

Therefore:

$$H(K|W, Y) = H(K) - H(Y|W) \quad (4)$$

And we know that:

$$H(K) = \log_2 \frac{Ns!}{(Ns - Nw)!} \quad (5)$$

Hence, the information leakage will be:

$$I(Y; K|W) = H(Y|W) \quad (6)$$

Security analysis for KOA scenario: If the opponent observes only watermarked content Y and its original version X, (Y, X), we have:

$$I(Y; K|X) = H(K|X) - H(K|X, Y) \quad (7)$$

Equivocation is indicated by H (K|X, Y)
We know that:

$$H(K|X, Y) = H(K|X, Y, W) \quad (8)$$

Then, we have:

$$H(K|X, Y, W) = H(K, X, Y, W) - H(W, X, Y) \quad (9)$$

We can write:

$$H(K, X, W, Y) = H(K, W, X) + H(Y|K, W, X) \quad (10)$$

In a clear way:

$$H(Y|K, W, X) = 0$$

Also, we know that:

$$H(Y, W, X) = H(Y|X, W) + H(X, W) \quad (11)$$

Therefore:

$$H(K|X, Y) = H(K) - H(Y|W, X) \quad (12)$$

We calculate this equivocation:

$$H(K|X, Y) = \log_2 \frac{-1\ 1}{P(Ns, Nw)\ P(Ns, Nw)} \quad (13)$$

P is the number of combinations of Ns taken *Nw* at a time. Hence, the information leakage in this case is:

$$I(Y; K|X) = H(Y|X, W) \quad (14)$$

Finally, if we assume that host image X and watermark W are independent, we will have:

$$I(Y; K|X) = H(Y|X) + H(Y|W) \quad (15)$$

Security analysis for WOA scenario: In this case, the opponent only has access to watermarked vector Y. There is a highest measure of uncertainty for opponent. The information leakage in the WOA scenario is:

$$I(K; Y) = H(K) - H(K|Y) \quad (16)$$

Equivocation is denoted by H (K|Y). First observe that:

$$H(K, W, Y) = H(W|Y, K) + H(K, Y) \quad (17)$$

It is clear that:

$$H(W|Y, K) = 0 \quad (18)$$

Because the opponent can extract the message easily by having access to the secret key and watermarked content. Hence:

$$H(K, Y) = H(K, W, Y) \quad (19)$$

Now we compute conditional entropy as follows:

$$H(K|Y) = H(K, Y) - H(Y)$$

$$= H(K, W, Y) - H(Y) \quad (20)$$

We know that:

$$H(K, W, Y) = H(Y|K, W) + H(K) + H(W) \quad (21)$$

Also, we know that: H (Y|K, W) = 0

Therefore, we have:

$$H(K|Y) = H(K) + H(W) - H(Y) \quad (22)$$

Then, the information leakage is:

$$I(Y; K) = H(Y) - H(K) \quad (23)$$

EXPERIMENTAL RESULTS

After the theoretical analysis carried out in previous section, this analysis is applied to multi resolution wavelet based watermarking techniques .Our goal is to evaluate the security level of wavelet based watermarking systems. This section calculates the information leakage and equivocation for different scenarios. Rationally, the threshold value T defined in QSWT algorithm is the most effective factor on the quantity of security.

Also, the robustness and imperceptibility in watermarked images are highly depending on the value of T. This threshold value determines the size of adequate set of wavelet coefficients for embedding the set of these wavelet coefficients that have called a QSWT in Hsieh *et al*. (2001). The smaller the threshold value T, the bigger the size of QSWT. Simulations have been conducted to evaluate the measure of security in the wavelet based watermarking methods. In the theoretical point of view, we expected to have raise in the measure of equivocation in all scenarios as a result of the increasing in the QSWT set. Moreover, it is predictable that by increasing the size of QSWT, the equivocation goes to the Shannon's limit of perfect secrecy. But, there are some fundamental limitations for the increasing of the equivocation from practical point of view. Figure 1 shows a comparison between the measure of equivocation in the WOA, KMA and KOA scenarios as a function of the size of QSWT. These measurements are calculated by the equivocation equations which were estimated in the previous section. It is not surprising that the security level against the WOA scenario is the highest. So, we conclude that in WOA scenario, getting information about the secret key will be

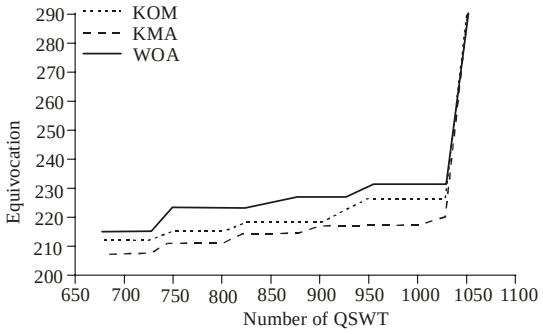


Fig. 1: The measure of equivocation for all scenarios

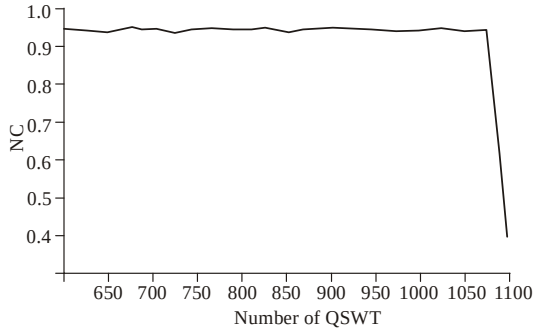


Fig. 2 Normalized correlation between the original watermark and watermark extracted.

Table 1: PSNR and information leakage for woa scenario

Image host	Threshold value	Ns	Information leakage (bit/sym)	PSNR (db)
Lena (512*512)	3	762	1.115	41.2626
Lena (512*512)	1	856	0.014	32.8764
Lena (512*512)	0.1	1233	0.0004	24.1267
Sydney (512*512)	3	987	1.523	40.2775
Sydney (512*512)	1	831	0.028	30.1986
Sydney (512*512)	0.1	1189	0.0011	24.0422

very difficult. In the KMA and KOA cases, the measure of equivocation is very close to each other and it is possible that the opponent is able to completely disclose the key, but it is highly dependent on the local characteristics of watermark and it varies from case to case. The important remark in Fig. 1 happens when the number of QSWT coefficients is bigger than 1050 where the measure of equivocation for all scenarios increases suddenly and drew on the ideal measure. This means that going on the high measures of equivocation by selecting a small value of T is possible but on the other hand it will cause other difficulties. To describe these problems, in Fig. 2, we depict the plot of normalized correlation as a function of size of QSWT. The normalized correlation is an indicator to assess quantitative similarity between the extracted watermark and the original watermark. We can see, the quantity of NC (Normalized correlation) decreases as the size of QSWT increases, especially for the number of QSWT bigger than 1050. It means that enhancement in the measure of security leads to a significant decrease in the robustness properties.

Furthermore, the visual imperceptibility of watermarking is measured by the Peak Signal to Noise Ratio (PSNR) of the host image and the watermarked image. Table 1 indicates the PSNR and information leakage in WOA scenario for the different threshold values T. It is clear that the cost of having very small values of information leakage is the vast reduce in PSNR. Hence, this reduce gives rise to a serious degrade in perceptual quality of watermarked image. This degrade is shown in Fig. 3.

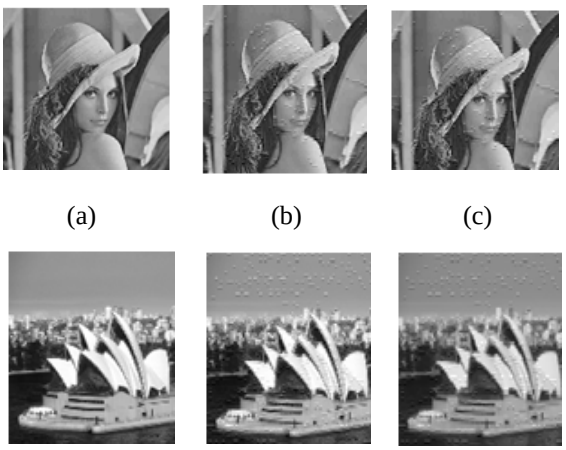


Fig. 3: Examples of watermarked image with different threshold value, where for (a) T = 1, (b) T = 0.1, (c) T = –1.

To sum up, there is a trade off between the security and other properties of a watermarking algorithm. Also, improvement in the security without any limitation can cause huge damages on other important characteristics of watermarking and it can be the main reason why achieving perfect secrecy defined by Shannon is impossible in practice. So, the appropriate threshold value is eligible based on the watermarking requirements. For example, based on the values in Table 1, T=1 can be an adequate threshold value to have a low information leakage with an acceptable PSNR and a desirable quality of watermarked image. This optimum threshold value can be different in other applications.

Watermarking with reed-Solomon coding: The section 4 illustrates a fundamental limitation to improving the security of watermarking schemes. The problem happened when water marker tried to increase the security level by picking up the small value of T. This problem related to a significant reduce in the robustness and imperceptibility of watermarking scheme where threshold value T is small. In this section, Reed-Solomon code is used to lighten this problem and improve the security level of watermarking systems. In communication systems, error correcting codes can help to achieve more efficient and reliable transmission. Reed-Solomon (RS) decoders can correct both errors and erasures. The erasures can be generated by a receiver that identifies the most unreliable symbols in a given codeword. When a receiver erases a symbol, it replaces the symbol with a zero and passes a flag to the decoder indicating that the symbol is an erasure, not a valid code symbol. . Since watermarking can be viewed as communication system, it is natural to use error

correcting codes to improve the detection precision and robustness. So we assessed the effect of using Reed-Solomon coding on the security of a water marking scheme. In this section, a Reed-Solomon code-based secure image water marking algorithm in DWT domain is proposed. Reed-Solomon codes are blocked-based error correcting codes. The algorithm takes advantage of the error correction capacity of Reed-Solomon codes to improve the robustness. Improving the robustness of algorithm as the cause of applying Reed-Solomon codes gives permission of choosing smaller values of T to water marker. It means that the security will increase without any remarkable reduce in the robustness.

Reed-Solomon coding: In this paper, the watermarked data is a gray image of size 36*36. We apply the code RS [36, *n*] to the watermark data. Where n denotes the block length of the RS code words. Before the embedding part of watermarking, watermark data is encoded with Reed-Solomon code. Reed-Solomon code is as follows:

Code = rsenc (msg, h, n)

where, n is the length of the RS code and *h* is the length of image watermark and *msg* is the matrix with *h* columns. Every row of *msg* is a code word. The Reed-Solomon code is in the form of a matrix with *n* columns. In this paper, the length of code *n* is 63 and the length of watermark rows *h* is 36. The sequence of code is denoted as A. The Reed-Solomon codes have a high error-correction capability and it was our motivation for using RS code in watermarking algorithm. The Reed-Solomon's decoder is able to correct (n-k/2 errors in each code word. Therefore, the code which we used in this study, can correct 13 errors in each code word.

Embedding algorithm: The procedure of embedding watermark is as follows.

Step 1: Decompose the original image *x* into three levels with ten sub-bands using three-level discrete wavelet transform:

C = {LL3, HL3, LH3, HH3, LL2… HH1}

Step 2: Sub bans LH3 is selected to be cast and threshold value T is chosen for finding QSWT coefficients which are appropriate for embedding watermark data.

Step 3: The random security key with the same size by the encoded watermark are created. Then, the security key K is used to identify the location of coefficients in QSWT which are going to be used for data embedding.

Step 4: The selected coefficients are modified with the pixels of encoded watermark:

$$v'(i, j) = v(i, j) + a^* A(l) \quad (24)$$

where, *v'*shows the transformed coefficients after embedding encoded watermark *A* in the wavelet coefficients *v*. Also, *a* is a scaling parameter for watermark embedding.

Step 5: The Inverse Discrete Wavelet Transform (IDWT) is applied to modified wavelet coefficients in order to produce the watermarked image.

Watermark extraction algorithm: The following are the steps in the extraction of the watermark:

Step 1: We first decompose a watermarked image *Y* and the original image x with discrete wavelet transform into three levels of ten sub-bands.

Step 2: Sub band LH3 is selected for extraction and the security key K is applied to determine the coefficients which are host for the pixels of encoded watermark. We subtract the same index of coefficients of sub band LH3 of *y '* by the coefficients of sub band LH3 of *y*.

Then we scale down the watermark:

$$W'(l) = (y'(i, j) - y(i, j)) / a. \quad (25)$$

Step 4: After arranging the index of watermarks, the extracted watermark is decoded using Reed-Solomon decoder.

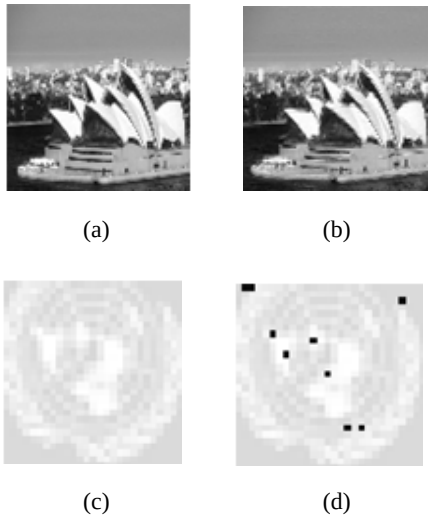
SIMULATION RESULTS AND COMPARISON

In the experiment, the original images of size 512*512 are used as the host images. We applied code RS (36, 63) on the 36*36 watermark images before embedding part of watermarking algorithm and wavelet decomposition is implemented by daubechies-4 wavelet based with 3 level. The purpose of this section is twofold: on one hand, we will analyse the practical effects of the proposed watermarking algorithm on tackling and lightening limitations which exist for increasing the security level of a watermarking system; on the other hand, we will make a comparison between security and robustness of proposed watermarking method which uses RS coding and simple QSWT watermarking algorithm.

We have provided in Fig. 4 and 5 the examples of watermarked images and their corresponding watermarks extracted. We can see that despite the increase in size of watermark image due to the applying RS code, quality

(a) (b) (c) (d)

Fig. 4: Example of watermarking with RS coding and T=1. (a) Original image, (b) watermarked image, (c) watermark, (d) extracted waterma



(a) (b)

(c) (d)

Fig. 5 Example of watermarking with RS coding and T = 1, (a) Original image, (b) watermarked image, (c) watermark, (d) extracted watermark.

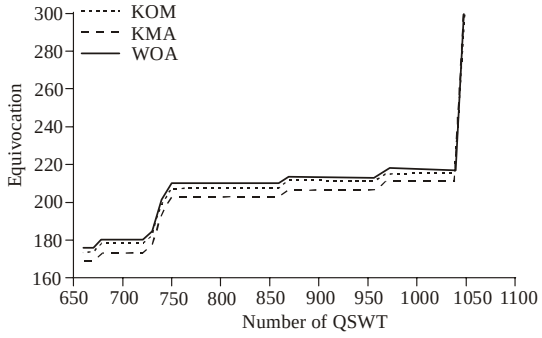


Fig. 6: The measure of equivocation of KMA, KOA, WOA scenarios with RS coding

reduction and obvious distortion is not visible in any of the watermarked images. Hence, it can be claimed that the quality of watermarked image is same for both of watermarking algorithms and using the RS code does not cause any considerable degradation in quality of watermarked image. The peak signal to noise ratio

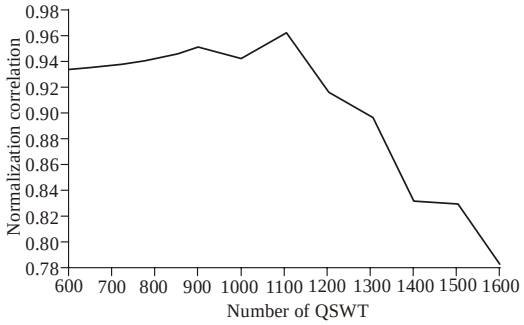


Fig. 7: Normalized correlation between the original watermark and watermark extracted for algorithm with using RS code

Table 2: PSNR for both watermarking algorithms

image Host	Threshold value	PSNR without coding (db)	PSNR with coding (db)
Lena (512*512)	3	41.2626	4.0.0128
Lena (512*512)	1	32.8764	33.5253
Lena (512*512)	0.15	24.1267	26.2811
Sydney (512*512)	3	40.2775	42.6748
Sydney (512*512)	1	30.1986	31.0138
5Sydney (512*512)	0.15	24.0422	25.4024
Sydney (512*512)	0.01	22.8541	22.1866

(PSNR) is used to evaluating the quality of the watermarked image. In order to compare this method with the method without using RS coding, the PSNR is calculated. Comparison results are shown in Table 2. The PSNR of all selected watermarked images are above 20 db. From the Table we can see that the both of watermarking methods are almost equivalent in the level of imperceptibility.

To assess the performance of proposed method from a security point of view, we plot the measure of equivocation for the method with RS coding as a function of the size of QSWT (Fig. 6). From Fig. 6, it is clear that the watermark size increase as a result of using RS coding, leads to the overall reduction in the amount of equivocation for opponent. The reason for this decrease is that with increasing the size of watermark, watermark image will be hidden in a larger number of QSWT coefficients and this can help the opponent for estimating the privacy data. For example, in the number of QSWT coefficients 800, the measure of equivocation for algorithm with using RS coding is 208 (bit/sym), whereas this value is 219 (bit/sym) when no code is used (Fig. 1). Also, approaching to Shannon's limit for perfect secrecy occurs in the greater number of QSWT in the algorithm with using RS code as compared to algorithm with no code. Thus, at first glance this seems that using RS code has a negative effect on the security level of watermarking system, but this is a wrong perception. With using the features of Fig. 7, we will indicate that the RS code can be

Table 3: Information leakage for woa scenario in two watermarking algorithms

NC with coding (bit/sym)	Host image	Threshold value	Ns	Information leakage without coding (bit/sym)	NC without coding (bit/sym)	Information leakage without coding (bit/sym)	NC with coding (bit/sym)
0.9418	Lena (512*512)	3	762	1.115	0.9554	2.0925	0.9418
0.9463MM	Lena (512*512)	1	856	0.041	0.9473	0.1086	0.9463
0.9529MM	Lena (512*512)	0.15	1080	0.0004	0.8127	0.0021	0.9529
0.9133MM	Sydney (512*512)	3	687	1.523	0.9272	1.817	0.9133
0.9427MM	Sydney (512*512)	1	831	0.02814	0.9396	0.04511	0.9427
0.9162MM	Sydney (512*512)	0.15	1083	0.0011	0.8244	0.0017	0.9162
0.8973MM	Sydney (512*512)	0.01	1368	0.00093	0.7085	0.00085	0.8973

used to improve the security level of watermarking system.

The normalized correlation (NC) between the extracted watermark and the original watermark is a significant criterion which determines the level of robustness for a watermarking algorithm. Figure 7 illustrates normalized correlation for algorithm with RS code as a function of number of QSWT. We can see that between the numbers of coefficient 500~1300, the measures of NC are appropriate and approximately stable. Then, the equivocation for method with using RS code reduced dramatically after the numbers of QSWT 1300 and as a result of this, algorithm will not be robust and utilizable, but from Fig. 2 we can see that for method with no code, this considerable decrease in the NC happens in the numbers of QSWT 1050. It means that the watermarker limitation for decreasing threshold value T and enhance security is number of QSWT 1300 in the method with using RS code and number of QSWT 1050 in the method with no code. If threshold value T further decreases, the security will improve while algorithm will not be applicable in practice. Furthermore, by comparing the amount of equivocation between both algorithms, it is obvious that the equivocation of the proposed method in the number of QSWT 1300 is very close to Shannon's limitation of perfect secrecy and higher than the equivocation of method with no code in the number of QSWT 1050.

Moreover, Table 3 indicates the quantity of information leakage for WOA scenario which is calculated from Eq. (23). It is clear that in the bigger values of T and smaller number of QSWT, the measure of information leakage in the no code scheme is smaller than scheme with using RS code, but with the lower threshold, the difference of the information leakage between two algorithms become smaller. Finally, in the threshold value 0.01 and numbers of QSWT 1368, we can see that method with no code is not useable because of low robustness whereas proposed method reached to a very little information leakage and reasonable measure of robustness.

Finally, we can conclude that the watermarker can access to upper security with applying Reed-Solomon code as an important factor to combat channel noise and improve the robustness of watermarking system.

CONCLUSION

This study pursued three important objectives. At first, the security of Wavelet-based data-hiding methods has been analysed from an information theory based point of view. Then, we have indicated that in the theory, security can be increased illimitable with abate in the threshold value T. As another purpose of this paper, after the theoretical analysis carried out in the first section, we evaluated the security for a wavelet-based watermarking algorithm which is called QSWT from a practical point of view and we have illustrated the practical problems which exist in the way to achieve Shannon's limitation for perfect secrecy. Eventually, the main objective of this paper was introducing a novel watermarking algorithm which increases the security level with using Reed-Solomon code. This is due to taking advantage of the error correction capacity of error correcting codes to improve the robustness.

Among the theoretical and practical results obtained in this study, we would like to remark on the following:

- In the theoretical side of this paper, we have provided a reliable estimation of security for different scenarios via tools of information theory which covers a wide range of wavelet-based watermarking schemes. In the practical side of the security problem, a trade off between security and robustness has been shown to exist in the watermarking methods and we have shown the difficulties which exist to achieve Shannon's limitation of perfect secrecy.
- In this paper, we present a novel watermarking algorithm for improving security level and robustness of wavelet based image watermarking. For the method studied in this paper, we use Reed-Solomon coding to robustly and securely hide watermark in the host image. The results show that the proposed algorithm has a good performance in certain practical scenarios. In particular, Reed-Solomon coding can significantly increase the security level when threshold value T is small.

- Nevertheless, we can not study the security in the digital watermarking as a separate issue because the different characteristics of digital watermarking are plenty relevant to each other. Therefore, we must analyse the security as an integral part of a set of interconnected properties.

REFERENCES

Bahat, V., I. Sengupta and A. Das, (2010). Audio watermarking based on BCH coding using CT and DWT. Int. Confer. Informat. Technol., pp: 49-52.

Barni, M., F. Bartolini and T. Furon, (2003). A general frame work for robust watermarking security. IEEE Trans. Signal Proc., 83(10): 2069-2083.

Cayre, F., C. Fontaine and T. Furon, (2005). Watermarking security: Theory and practice. IEEE Trans. Signal Proc., 53(10): 3976-3987.

Cayre, F. and P. Bass, (2008). Kerckhoffs based embedding security class for WOA data hiding. IEEE Trans. Signal Proc., 3 (1): 1-15.

Cheng Liu, S., Shi-Feng and D.Lin, (2006). BCH Code_Based Robust Audio Watermarking. J. Informat. Sci. Eng., 22(23): 535-543.

Comesana, P., F. Perez-Gonzalez and F. Balado, (2006). Watermarking security: A survey. IEEE Trans. Signal Proc., 54(2): 585-600.

Hsieh, M., D. Tseng and Y. Huang, (2001). Hiding digital watermarks using multiresolution wavelet transform. IEEE Trans. Signal Proc., 48(5): 875-881.

Kalker, T., (2001). Consideration on watermarking security. IEEE Int. Workshop Multimedia Signal Process., 20 (18): 201-206.

Kutter, M., S. Voloshynovskiy, A. Herrigel and P.W. Wong, (2001). Watermark copy attack. Proc. SPEI Security Watermark. J., 39(4): 88-94.

Moulin, P., (2001). The role of information theory in watermarking and its application to image watermarking. IEEE Trans. Signal Proc., 81(12): 1121-1139.

Simmons, G., (1984). The prisoners problem and the subliminal channel. Proc. Adv. Cryptol., 5 (2): 51-67.

Wang, Y.A., (2004). Steganalysis of block-structured stegotext. Proc. Security Stenograp. Watermark. Multimedia Contents., 53(6): 477-483.