A Novel JFD Scheme for DRM Systems Based on DWT and Collusion Resistance Fingerprint Encoding

Reham Mostafa[1], Hamdy El-Minir[2], and Alaa El-Din Mohamed[1]
[1]Faculty of Computer and Information Science, Mansoura University, Egypt
[2]Faculty of Engineering, Kafr El-Sheikh University, Egypt

Abstract: *With the proliferation of the internet and rapid development of multimedia, media distribution and traitor tracing issues have become imperative and critical. In this paper, the Digital Rights Management (DRM) system based on novel Joint Fingerprinting and Decryption (JFD) scheme is proposed, which transmit the encrypted image to different customers and makes each customer decrypt the image into a different copy that contains the customer's unique information. Till now, some JFD schemes have been reported, that solves encryption and fingerprinting simultaneously and has high efficiency, but several problems still remain to be tackled in JFD, including poor encryption security, severe fingerprinted image distortion, etc. An improved JFD scheme, which based on Discrete Wavelet Transform (DWT) of media and collusion resistant fingerprint encoding, is presented in the paper. The experimental results show that the proposed scheme is more secure compared with the existing scheme, it obtains good imperceptibility and robustness. These properties make it a suitable choice for secure image distribution in real time applications.*

Keywords: *DRM, JFD, traitor tracing, DWT, partial encryption*.

Received April 30, 2014; accepted October 19, 2015

1. Introduction

With the rapid development of information and communication technologies, users could access to digital resources and services in anytime, at anywhere, which is much easier than ever before. Under these conditions, the copyright infringement, such as a free distribution, unauthorized usage, illicit sharing of copyrighted digital contents, will be a common phenomenon. Consequently, the digital contents industry could be heavily damaged, and its value chain may also be interrupted. Digital Rights Management (DRM) systems were created to protect high-value digital contents and control their distribution and usage.

In order to protect DRM system from tampering, hardware based protection is used, which predominantly implemented in set-top boxes. There are many disadvantages such as the inflexibility and high cost. It requires a large investment cost from the service provider and increases time to market. At a time where a lot of pirated content is available on the Internet, hardware-based solutions are not valuable for the consumer.

In order to reduce the investment cost, the software-based DRM [6, 10] is proposed in exchange for hardware-based DRM. The biggest advantage of software-based DRM is that they can cheaply be distributed to the customers via networks and does not need to create additional per-installation costs.

Even though the encryption and watermarking techniques achieved great success in protecting some properties of multimedia data such as confidentiality, integrity, and ownership, software-based DRM systems, such as Internet Streaming Media Alliance (ISMA) [8], Advanced Access Content System (AACS) [1, 17], are assumed to be insecure. Especially, such kind of software-based DRM technologies are manipulated by encryption and watermark method separately. Therefore, the original content is exposed temporarily inside a system in the user's decryption.

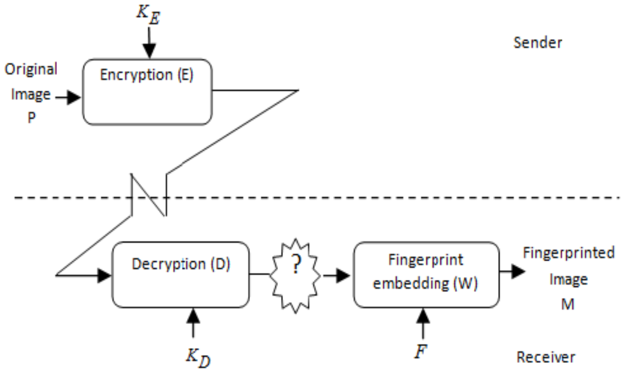


Figure 1. General architecture of secure media distribution [16].

In that case, users can save original contents from the gap between the decryption and fingerprinting operations without watermark information and distribute via network as shown in Figure 1 the decryption and fingerprint embedding process is defined as:

$$M = W\left(D(C,K_D),F\right) \tag{1}$$

Where *C*, $K_D F$, $K_D F$, *M*, *D*( ), and *W*( ) are the encrypted-media, decryption key, fingerprint information, fingerprinted media, decryption function and fingerprint embedding, respectively.

To solve the problem of content leakage, a Joint Fingerprinting and Decryption scheme (JFD) [3] scheme was proposed as shown in Figure 2 In the JFD scheme, the decryption and fingerprinting processes work simultaneously which avoids the gap between decryption and fingerprint embedding and improves the security of embedding fingerprint at the customer side. The JFD operation is defined as:

$$M = J\left(C,K_D,F\right) \tag{2}$$

Where *C*, K_D *F*, *M* and *J*( ), are the encrypted-media, decryption key, fingerprint information, fingerprinted media and JFD function, respectively.

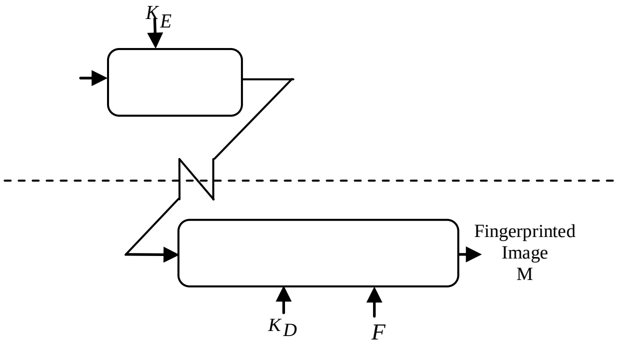


Figure 2. Secure media distribution based on JFD [16].

For it implements both watermarking and decryption operations, the properties belonging to both watermarking and encryption should be satisfied, which are list as below:

- Security against cryptographic attacks (statistical attacks, brute-force attacks, etc.).
- Security against collusion attacks.
- Robustness against signal processing (additive noise, compression, filtering, etc.).
- Imperceptibility of fingerprint.
- Efficiency in implementation.

Till now, several JFD schemes have been proposed [3, 12, 13, 16] to joint fingerprint embedding and decryption to obtain a trade off between security and efficiency. However, since the combination of encryption and watermarking is still an open issue in these schemes, some contradictions are still not solved, such as the relation between security, robustness and imperceptibility, etc. Additionally, the security against the biggest threaten, named collusion attack, is not considered by these schemes.

In this paper, we review the existing schemes that joint fingerprint embedding and decryption, and analyze their properties. With respect to their disadvantages, we describe a design and implementation of DRM system based on a novel JFD scheme. The proposed JFD scheme is based on Discrete Wavelet Transform (DWT) of content and collusion resistant fingerprint encoding. Two features of the proposed JFD scheme make itself a suitable approach for protecting copyright of multicast media on the Internet. These features are:

1. Effective transmission. All the data, including encrypted contents, can be transmitted with the multicast method. Only the decryption keys need to be delivered with the unicast method.
2. Security and imperceptibility. When an image is encrypted, the most significant transform domain coefficients are encrypted such that it has little or no commercial value. On the other hand, a decrypted image left only a few coefficients that are still encrypted which contain the fingerprint, causes only imperceptible degradation in image quality.

The rest of the paper is organized as follows: Section 2 presents an overview of related works on JFD scheme. Section 3 proposes a fundamental idea of DRM system based on JFD scheme. Section 4 introduces the DWT. Section 5 details the proposed JFD scheme based on DWT of image. Experimental results are presented in section 6. Finally, in section 7, we summarize the proposed method and draw a brief concluding remark.

2. Related Work

Till now several JFD schemes have been proposed, which are analyzed as follows.

Anderson and Manifavas [3] proposed the Chameleon method based on table lookup operations, which provided good imperceptibility for the fingerprinted data. The method encrypts media data with a stream cipher at the server side, distributes the data, decrypts and fingerprints the media data by modifying the Least Significant Bits (LSB) under the control of different decryption key. This scheme is secure in cryptographic aspects, but is not robust to signal processing, such as recompression, noise, etc.

Kundur and Karthik [11] proposed a classic architecture JFD scheme based on partial decryption, which encrypts signs of Discrete Cosine Transform (DCT) coefficients of the media on the sender side and then decrypts them partially according to the user's fingerprint on the receiver side. The scheme is robust to some operations, while the imperceptibility cannot be confirmed, the encrypted media content is not secure in perception and the security against collusion attacks cannot be confirmed.

Lian *et al.* [14] proposed the JFD scheme that encrypts media data at the server side by additive modulation, and decrypts media data at the customer side by controllable demodulation under the control of the fingerprint codes. The scheme is robust to some operations that benefit from watermarking algorithms' properties, while the security against cryptographic attacks and collusion attacks cannot be confirmed.

Lemma *et al*. [12] also proposed a JFD method based on homomorphic operations. The media data is to achieve encryption and decryption by means of different key streams. Each key stream has the same size as the media, leading to prohibitive transmission costs. The scheme is secure against cryptographic attacks that benefit from encryption algorithms' properties, while the transmission of key stream costs much time and space. Additionally, the security against collusion attacks is not emphasized. A generalized version of Lemma's method has been proposed by Celik *et al*. [5], which not only reduces transmission costs but also provides an efficient fingerprint detection method and rigorous security proofs.

Huang and Chen [7] propose a new JFD method based on Genetic Algorithms (GA). The method first generates encryption and decryption keys with GA. Multimedia data is then encrypted and transmitted to all users. At the same time, a secure channel is used to send decryption key to each user. When a user employs the designated key to decrypt the received video, a designated fingerprint would be embedded into the video. The method can transmit media data to clients effectively and cause only a slight degradation in perceptual quality. Moreover, the method has the capability to resist some attack methods if an appropriate encryption method is adopted.

Xu *et al*. [20] also proposed a JFD method based on selective content encryption to enhance encryption security. In order to further reduce partial decryption's influence on image quality, they use the structural distortion as a measurement to choose fingerprint embedding area. The scheme is provide a fingerprinted image that still has good quality after high secure selective content encryption and partial decryption, but the security against cryptographic attack and collusion attack cannot be confirmed.

Lian and Chen [13] propose a JFD scheme based on homomorphic encryption and watermarking operations. Because the encryption algorithm and fingerprinting algorithm are homomorphic, their properties, such as security, collusion resistance and robustness are kept unchanged. The scheme is robust against collusion attack, while the robustness against some other operation (filtering, re-sample, rotation, etc.) cannot be confirmed.

According to the above analysis, there are still some disadvantages in the existing schemes, especially the fragileness to collusion attacks. That is caused by two reasons, i.e., the encryption and watermarking operations are not combined suitably and the collusion-resistant fingerprint encoding method is not adopted in the JFD schemes. For these reasons, we propose a novel JFD scheme based on DWT of content and collusion resistant fingerprint encoding to overcome these defeats.

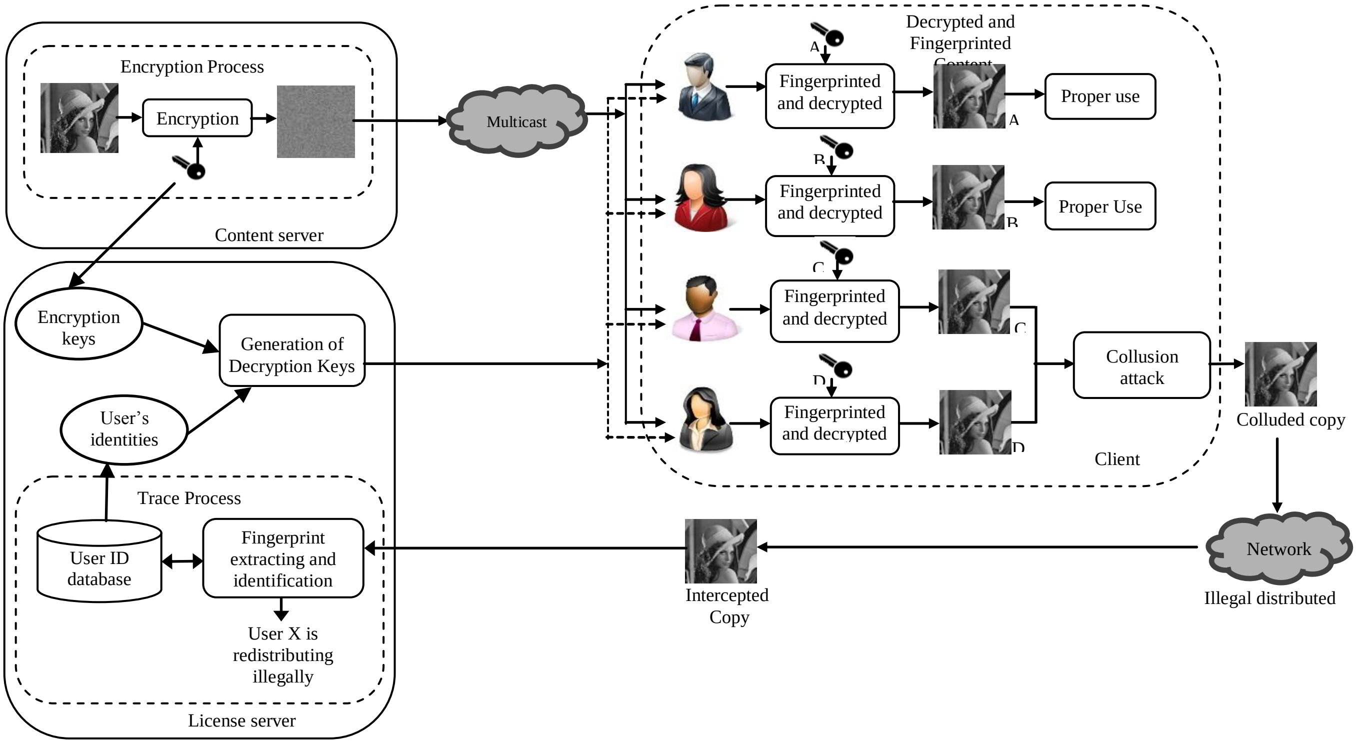


Figure 3. Architecture of DRM system based on JFD scheme.

3. The Proposed Architecture of Joint Fingerprinting And Decryption System Based on Joint Fingerprinting And Decryption Scheme

The idea of the DRM system based on the JFD method is presented in this subsection. A DRM system requires to enable the distribution of original contents safely and smoothly, as well as to enable the secondary use of contents under rightful consents. When a DRM system is constructed using the JFD scheme to implement a content distribution system, it is not only the safety distribution method to users, but also the solution of the conventional DRM problem.

As shown in the Figure 3, the components of DRM system are typically divided between the server at the content provider, the server at the DRM service provider, and the hardware at the consumer site. In the content provider side, only one copy of data is encrypted using common group key. This copy is sent through multicast transmission to all registered users, so that bandwidth required to work the system and the number of connections is kept constant and independent of the number of customers. In the DRM service provider side; there is a set of unique decryption keys for each user, which are sent to them through unicast transmissions.

At consumer side, the encrypted media is decrypted and embedded with fingerprint, so that sender side doesn’t have to perform many complicated operations. Unlike the previous strategy, encryption is an integral part of the fingerprinting method. Decryption keys are constructed so that decryption introduces changes in media. These changes are unique for all the users and are imperceptible to the human, so these changes are fingerprints. These properties provide high scalability, which is extremely important in multimedia distribution systems. In this paper, we propose a JFD scheme based on DWT of the media. The proposed JFD uses DWT, is largely based on the following observations:

- *Observation 1*. A large majority of useful image contents change relatively slowly across images. By converting the image into the spatial frequency domain; it says that, lower spatial frequency components contain more information than the high frequency components which often correspond to less useful details and noises.
- *Observation 2*. Psychophysical experiments suggest that human’s eyes are more sensitive to loss of lower frequency components than loss of higher frequency components.

4. Review of Discrete Wavelet Transform

DWT [9] is a mathematical tool for hierarchically decomposing an image wavelet transform provides both frequency and spatial description of an image. In two-dimensional DWT, each level of decomposition produces four bands of data, one corresponding to the Low Level (LL) pass band, and three other corresponding to Horizontal (HL), Vertical (LH), and diagonal (HH) high pass bands. The decomposed image shows an approximation image in the lowest resolution low pass band, and three detail images in higher bands.

The low pass band can further be decomposed to obtain another level of decomposition. The three-level DWT decomposition is shown in Figure 4. The Human Visual System (HVS) [2] is more sensitive to low-frequency coefficients, and less sensitive to high frequency coefficients.

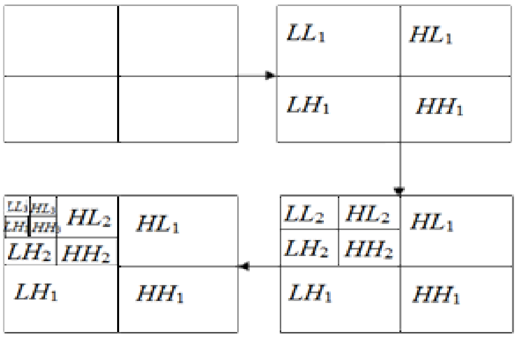


Figure 4. Flow of DWT process (3-level decomposition).

5. The Proposed Joint Fingerprinting And Decryption Scheme Based on Discrete Wavelet Transform

Attempting to overcome JFD’s problems, we will present an improved JFD scheme which inherits JFD scheme’s high efficiency and overcomes its shortcomings by many ways. That is, a new encryption strategy based on partial content encryption is proposed to enhance encryption security and reduce computational requirement for encryption in JFD; a DWT based frequency domain watermarking is proposed to identify the areas in the host image where a watermark can be embedded effectively that make the watermark visually imperceptible and robust against attack; finally, the collusion resistant fingerprint encoding are proposed to improve the JFD scheme’s performance against collusion attacks. By these ways, JFD’s problems can be solved in order to enable it suits for the content security protection of visual media. The proposed JFD schema is shown in the Figure 5.

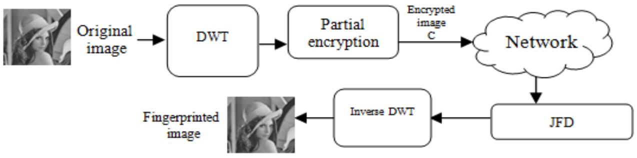


Figure 5. Architecture of the proposed JFD.

To implement our proposed JFD scheme, the hill cast method [18] that is belongs to the group of JFD methods has been chosen. The method provides a cryptographic security and digital fingerprinting of multimedia content, while maintaining high scalability.

5.1. Partial Image Encryption based on Discrete Wavelet Transform

The encryption scheme presented here is based on the DWT as shown in Figure 6. The scheme aims at reducing encryption time by only encrypting the significant part of the image, likewise maintaining a high level of security by shuffling the rest of the image using the Shuffling Algorithm.

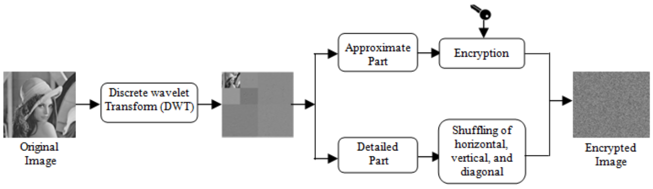

Original Image
Discrete wavelet Transform (DWT)
Approximate Part
Encryption
Detailed Part
Shuffling of horizontal, vertical, and diagonal
Encrypted Image

Figure 6. Block diagram of encryption process.

Algorithm: in the DWT method, the image first goes through the single-level DWT resulting in four coefficient matrices; the approximation LL, HL, LH, and HH matrices as discussed previously and shown in Figure 4. The lowest frequency sub band is expressed in the matrix LL. The LL matrix will be encrypted as it holds most of the image's information. For encryption, cipher text Y is obtained by multiplying the LL matrix (noted as X) by an encryption key matrix equation:

$$Y=XE \bmod 256 \tag{3}$$

Where all three matrixes are of size nxn and elements of these matrixes have values from 0 to 255. The key matrix E must be modular invertible.

While encrypting this matrix alone will provide complete perceptual encryption, it would be possible for an attacker to gain information about the image from the other matrices. Therefore, the HL, and HH matrices will be shuffled. The Shuffling Algorithm used in the DCT method is used here. The encrypted LL matrix and the shuffled HL, LH and HH matrices then grouped together to produce the encrypted image. Figure 6, shows the block diagram of the encryption process.

5.2. Selection of Fingerprint Embedding Area

In this paper, LL sub band has selected for watermark embedding as it contain most energy of image. Low frequency coefficients are nearly unchanged to common attack so that watermarking information embedded in low frequency coefficients has better robustness.

5.3. Joint Fingerprint and Decryption

To implement JFD scheme, it's necessary to provide a unique key (unique fingerprint) for each user. The user's unique fingerprint F must be associated with decryption key D in the following way:

$$D = E^{-1}\left(1+\alpha F\right) \tag{4}$$

Where α is the perception coefficient and is selected in such a way that the watermarked image remain perceptually unaltered. The matrix E^{-1} is the modular inverse of the matrix E.

When the user receiving the encrypted media Y, he uses his key D to obtain a watermarked copy X_D. The following formula is used to perform JFD is:

$$X_D = \lfloor YDmod256 \rfloor \tag{5}$$

Then reshuffle the HL, LH, HH sub bands to return them into their original locations, and combine them with X_D to get the watermarked image.

5.4. Extraction of Fingerprint and Traitor Tracing

The extraction of fingerprint from the intercepted copy $X_{colluded}$ is realized at the distribution side with coherent detection. The extraction may be conducted using the following formula:

$$w' = \frac{1}{\alpha}\left(X_{colluded} - X\right) \tag{6}$$

Where w' is the extracted fingerprint that used to identify the pirate or the illegal distributer. We correlate w' with each user's fingerprint sequence w_i using Equation 7:

$$T_n\left(i\right) = \frac{w' w_i}{\sqrt{\left\|w_i\right\|^2}}\; i = 1, 2, ..., n \tag{7}$$

The colluder is the user whose fingerprint has the highest correlation value $T_n(i)$.

5.5. Robustness Against Collusion Attack

One cost-effective strategy to attack digital fingerprint is collusion, where several colluders can combine their individuals copies with collusion operation (min-max selection, averaging, linear combinatorial collusion attack, etc.) in order to disrupt fingerprint.

In the proposed JFD scheme, the media copy corresponding to different customer is identified by different fingerprint sequence. The fingerprint sequence is generated by pseudorandom sequence generators, which is not secure against collusion attack. To resist the proposed JFD scheme against collusion attack, the fingerprint sequence can be encoded with some collusion resistant codes, such as

Boneh and Shaw [4] code, Wu *et al*. [20] code and Tardos [19] code.

In these fingerprint coding methods, the fingerprint sequence will be generated according to two steps: First, according to the customer's order, e.g., User ID, the fingerprint code: Q = q_0, q_1, …, 1_k q_j = 0 or 1, j=0, 1, ..., K-1 is generated with the collusion-resistant codes [4, 19, 20]. Second, the fingerprint code Q is modulated with spread spectrum method and produces the fingerprint sequence w=*w*0, *w*1, …, w_{n-1}. The sequence will be embedded according to Equation 5.

6. The Experimental Result and Analysis

The experiment included three parts: A performance analysis of the encryption, imperceptibility of the fingerprints, and robustness of the fingerprints.

6.1. Performance Analysis of Encryption

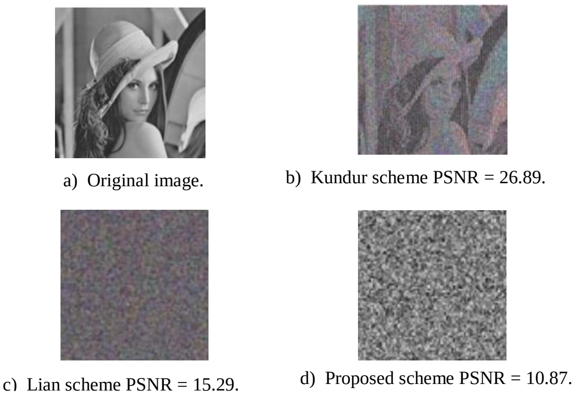
The performance of the proposed encryption method was analyzed from the standpoint of perceptual security and cryptographic security.

6.1.1. Perceptual security

The proposed scheme, Kundur and Karthik [11] scheme, and Lian *et al*. [14] scheme are used to encrypt the 512×512 Lena image, respectively. Schemes in [11, 14] based on DCT transform of image, while our proposed scheme is based on DWT transform of image. Perceptual security was evaluated by the *PSNR* value which is defined as follow:

$$PSNR = 10 \times log10\left(255^{2}/MSE\right) \tag{8}$$

Where MSE denotes the mean square error between the original image and the encrypted image.



a) Original image.

b) Kundur scheme PSNR = 26.89.

c) Lian scheme PSNR = 15.29.

d) Proposed scheme PSNR = 10.87.

Figure 7. Encrypted image quality.

Generally, the lower value of PSNR represents better encryption quality and the higher the perceptual security. The encryption results are shown in Figure 7. From this figure, we can see that the proposed scheme has a higher perceptual security than the other two schemes. This is because Kundur and Karthik [11] scheme encrypts only the sign of the DCT coefficients; therefore, perceptual security is poor. Lian and Chen [13] scheme encrypts the DC coefficients and the sign of the AC coefficients in DCT transform; thus, it obtains a higher perceptual security than Kundur and Karthik [11] scheme. Our proposed scheme encrypts LL sub band that holds most of the image's information in DWT transform of image while shuffling the HL, LH, and HH sub band.

Table 1 shows the comparative results of encryption with different size of images. The results show that Lian *et al*. [14] scheme has better security than Kundur and Karthik [11] scheme, while our proposed scheme obtains better perceptual security than the other two schemes.

Table 1. Comparison of the encrypted image quality.

Image	Encrypted image Quality (PSNR)			Recovered image Quality (PSNR)		
	Kundur	Lian's	Proposed	Kundur	Lian's	proposed
Airplane	12.8811	10.9257	9.3566	15.2348	12.0032	9.0931
Tank	13.9237	11.9051	9.3016	17.2178	14.9271	11.9102
Airport	14.5307	12.8002	11.3566	21.8811	16.9257	14.0011

6.1.2. Cryptographic Security

To test the cryptographic security we use the histogram analysis, information theory analysis, and correlation coefficient analysis.

- *Histogram Analysis:* Figure 8 describes histogram analysis; it shows histogram of plain image and the histogram of cipher image. It is clearly visible that histogram of cipher image is flat or uniformly distributed and it does not leak any amount of information about the plain image. Therefore the proposed encryption technique is secure from frequency analysis attack.
- *Information Entropy Analysis:* Information entropy is used to express the degree of uncertainties in the system. It is well known that the entropy *H*(*x*) of a message source *m* can be calculated as:

$$\begin{aligned} H\left(x\right) &= \sum_{i=1}^{n} p\left(x_i\right) I\left(x_i\right) = \sum_{i=1}^{n} p\left(x_i\right) log_b\left(\frac{1}{p\left(x_i\right)}\right) \\ &= -\sum_{i=1}^{n} p\left(x_i\right) log_b\left(p\left(x_i\right)\right) \end{aligned} \tag{9}$$

Where $p(x_i)$ represents the probability of symbol x_i and the entropy is expressed in bits. If each symbol has an equal probability then entropy of 8 would correspond to complete randomness, which is expected in encrypted image.

Table 2. Image entropy.

File Description	Size	Entropy Value	
		Encrypted Image	Original Image
Airplane	256×256	7.6453	7.7335
Tank	512×512	7.7894	7.7565
Airport	1024×1024	7.8936	7.7545

Table 2 shows the entropy value of the original image and encrypted image. Entropy analysis shows that the proposed encryption algorithm has entropy that close to ideal entropy (8), this implies that information leakage in the encryption process is fiddling and the encryption system is able to resist the entropy attack.

Correlation Coefficients Analysis: There is a high correlation between adjacent pixels in the image data. Correlation is a measure that computes degree of similarity between two adjacent pixels in horizontal, vertical and diagonal orientations.

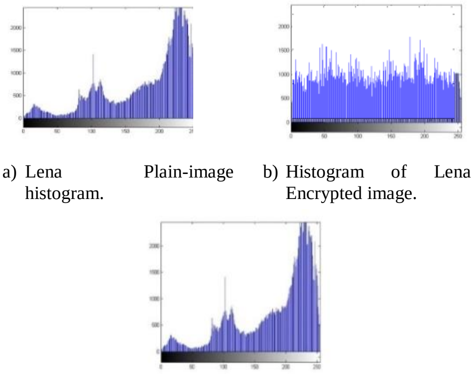
$$\tau = \frac{\sum_{i=1}^{n}\left(x_i - \bar{x}\right)\left(y_i - \bar{y}\right)}{\sqrt{\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2}\sqrt{\sum_{i=1}^{n}\left(y_i - \bar{y}\right)^2}} \tag{10}$$

Where x and y are gray level values of two adjacent pixels in the image and N is the number of adjacent pixels selected from the image to calculate the correlation.

Correlation test image is shown in Figure 7-a. Figure 9 shows the correlation distribution of two adjacent pixels in the plain image and cipher-image. It is observed that encryption algorithm is good because it hides all attributes of plaintext image, and encryption image is totally random and high uncorrelated. Results of correlation coefficient are shown in Table 3.

Table 3. Correlation coefficients of two adjacent pixels.

File Description	Size		Correlation Coefficient Analysis	
			Adjacent pixels orientation	
			Horizontal	Vertical
Airplane	256 × 256	Original image	0.8915	0.9621
		Encrypted image	-0.0486	0.0232
Tank	512 × 512	Original image	0.9795	0.9521
		Encrypted image	-0.0495	0.0697
Airport	1024 × 1024	Original image	0.9661	0.9887
		Encrypted image	0.0050	0.0619

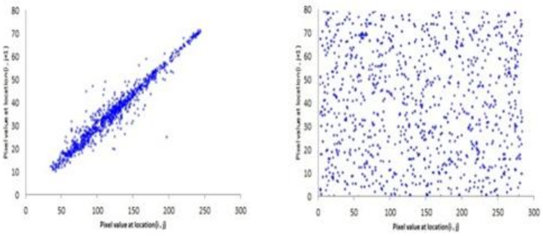


a) Lena Plain-image histogram.

b) Histogram of Lena partial Encrypted image.

c) Histogram of Decrypted image

Figure 8. Histogram of plain-image and partial encrypted image.



a) Plain Image.

b) Cipher Image.

Figure 9. Correlation of two adjacent pixels.

6.2. Imperceptibility of Fingerprint Embedding

Figure 10 shows a comparison of a fingerprinted image generated by different methods. As seen in the figure, our scheme obtains better image quality after fingerprint embedding. In our scheme, the fingerprint is embedded in the lower frequency sub band (LL), which has a smaller effect on the image quality; therefore, the fingerprint is embedded imperceptibly. But in Kundur's scheme, the fingerprint is generated by partially decrypting the sign bit of the AC coefficients, which affects the image quality in an obvious manner; in Lian's scheme, the fingerprint is embedded in the DC coefficient by decrypting under the control of the key and fingerprint, and the change in the DC coefficient also degrades the image quality in an evident fashion; and the degradation of Kundur's scheme is stronger than Lian et al's scheme.

The imperceptibility of watermarked image is qualitatively decided by visual artefacts in watermarked image. As a quantitative measure, following metrics are used:

- *Peak Signal to Noise Ratio (PSNR):* is calculated between the original and the watermarked image. Larger the PSNR value, more similar is watermarked image to the original image. If the PSNR value is greater than 30dB then the perceptual quality is acceptable.
- *Similarity Factor (SF):* The similarity factor determines the similarity of pixel intensities between the original image and the watermarked image. This helps us to calculate the changes in the perceptual quality of the image more precisely. The formula for SF is shown below:

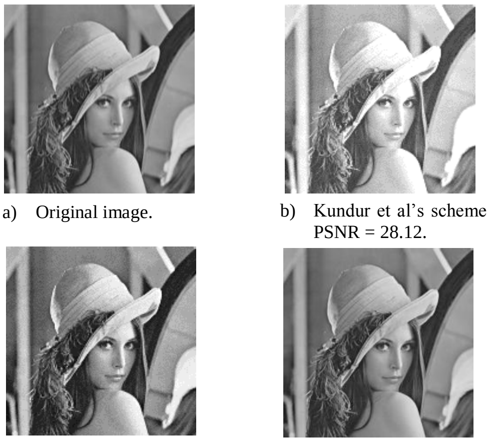
$$SF = \frac{\sum_i \sum_j x\left(i,j\right) * x'\left(i,j\right)}{\sum_i \sum_j x'\left(i,j\right)^2} \tag{11}$$

Where X (i, j) is the original image, and $X'(i, j)$ is the watermarked image. The similarity factor is approximately nearer to 1 for better imperceptible image quality.

Table 4 shows the comparative results of fingerprint embedding with different size of images. The results show that Lian's scheme has better watermarked image quality than Kundur's scheme, while our proposed scheme obtains better watermarked image quality than the other two schemes.

Table 4. Comparison of the fingerprinted Image quality.

Image	watermarked Image Quality PSNR			Watermarked Image Quality IF		
	Kundur	Lian's	Proposed	Kundur	Lian's	Proposed
Airplane	30.4346	36.0028	49.1266	0.9234	0.9536	0.9762
Tank	27.9301	34.4051	46.3982	0.9238	0.9602	0.9810
Airport	26.9901	33.0289	45.3001	0.9321	0.9712	0.9896


a) Original image.

b) Kundur et al's scheme PSNR = 28.12.

c) Lian et al's scheme PSNR=35.01.

d) Proposed scheme PSNR=49.15.

Figure 10. Imperceptibility of fingerprinting image.

6.3. Collusion Resistance of Fingerprint

To test the improved scheme against collusion attack, we test the detection rate under different number of colluders as shown in Figure 11. In this experiment, the total number of customer is 100, the number of colluders range from 2 to 50, and the tested fingerprint codes are Boneh-Shaw code [4], Wu et al's code [20] and Tardos code [19]. As can be seen, the improved scheme with various fingerprint codes obtains high detection rate when the number of colluders is certain.

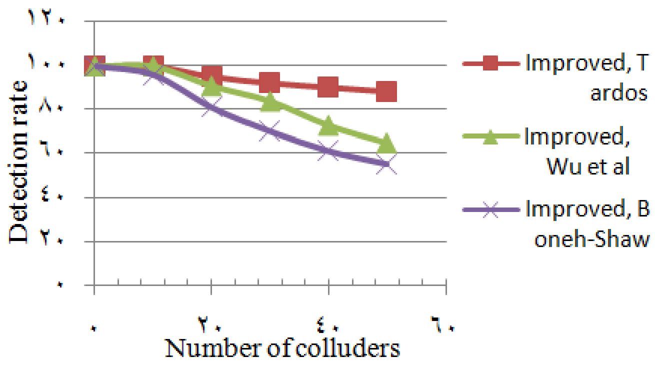


Figure 11. Comparison of collusion resistance.

7. Conclusions and Future Works

In this paper, we have presented the architecture of DRM system based on JFD scheme, by doing so; we can eliminate the problem of the present DRM technology and manage the legal user effectively. We also have proposed a novel JFD scheme that based on DWT of content and collusion resistant fingerprint encoding.

Experimental results demonstrate that the proposed scheme can transmit media data to clients effectively and the encrypted image is perceptually unintelligible as it gives the lowest PSNR value compared with another JFD scheme. With regard to watermarked image quality, it causes only a slight degradation in perceptual quality. Moreover, the proposed method has the capability to resist collusion attack methods by using different collusion resistance fingerprint encoding.

In the future works, our method can be applied on the compression digital content format using DWT based coders such as JPeG2000, SPIHT and so on. In addition, our proposal can be extended to other areas, such as multimedia streaming video.

References

[1] Advanced access content system (AACS) technical overview, http://www.aacsla.com, Last Visited 2013.

[2] Abbasi A., Seng W., and Ahmed I., "Multi Block Based Image Watermarking in Wavelet Domain Using Genetic Programming," *The International Arab Journal of Information Technology*, vol. 11, no. 6, pp. 582-589, 2014.

[3] Anderson R. and Manifavas C., "Chameleon - A New Kind of Stream Cipher," *in Proceeding of the 4th International Workshop on Fast Software Encryption*, pp. 107-113, 1997.

[4] Boneh D. and Shaw J., "Collusion-Secure Fingerprinting for Digital Data," *IEEE Transaction of Information Theory*, vol. 44, no. 5, pp. 1897-1905, 1998.

[5] Celik M., Lemma A., Katzenbeisser S., and Veen M., "Look-up Table Based Secure Client-Side Embedding for Spread Spectrum Watermarks," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 475-487, 2008.

[6] Emmanuel S. and Kankanhalli M., "A Digital Rights Management Scheme for Broadcast Video," *Multimedia System*, vol. 8, no. 6, pp. 444-458, 2003.

[7] Huang H. and Chen Y., "Genetic Fingerprinting for Copyright Protection of Multicast Media," *Soft Computing*, vol. 13, no. 4, pp. 383-391, 2010.

[8] Internet streaming media alliance implementation specification 2.0, http://www.isma.tv, Last Visited 2013.

[9] Kashyap N. and SINHA G., "Image Watermarking using 3-Level Discrete Wavelet Transform (DWT)," *International journal of Modern Education and Computer Science*, vol. 3, pp. 50-56, 2012.

[10] Kirovski D., Peinado M., and Petitcolas F., "Digital Rights Management for Ddigital Cinema," *International Symposium on Optical Science and Technology*, vol. 9, no. 3, pp. 228-238, 2001.

[11] Kundur D. and Karthik K., "Video Fingerprinting and Encryption Principles for Digital Rights Management," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 918-932, 2004.

[12] Lemma A., Katzenbeisser S., Celik M., and Veen M., "Secure Watermark Embedding Through

Partial Encryption," *Lecture Notes in Computer Science*, vol. 4283, pp. 433-445, 2006.

[13] Lian S. and Chen X., "Lightweight Secure Multimedia Distribution Based on Homomorphic Operations," *Telecommunication System*, vol. 49, no. 2, pp. 187-197, 2012.

[14] Lian S., Liu Z., Ren Z., and Wang H., "Secure Distribution Scheme for Compressed Data Streams," *in Proceeding of IEEE International Conference on Image Processing ICIP*, pp. 1953-1956, 2006.

[15] Lin C., Huang W., and Chen T., "Noise-Resistant Joint Fingerprinting and Decryption Based on Vector Quantization," *in Proceeding of IEEE International Conference on Broadband, Wireless Computing, Communication and Applications*, Fukuoka, pp. 463-468, 2010.

[16] Lin C., Prangjarote P., Kang L., Huang W., and Chen T., "Joint Fingerprinting and Decryption with Noise-Resistant for Vector Qquantization Images," *Signal Processing*, vol. 92, pp. 2159-2171, 2012.

[17] OMA, Open mobile alliance specification version 2.0, http://www.openmobilealliance.org, Last Visited 2013.

[18] Rykaczewski R., "Hillcast-A Method of Joint Decryption and Fingerprinting for Multicast Distribution of Multimedia Data," *Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics Annals, series Information Technology*, 2010.

[19] Tardos G., "Optimal Probabilistic Fingerprint Codes," *in Proceeding of the 35th Annual ACM Symposium on Theory of Computing*, San Diego, pp. 116-125, 2003.

[20] Wu M., Trappe W., Wang Z., and Liu R., "Collusion-Resistant Fingerprinting for Multimedia," *IEEE Signal Processing Magazine*, vol. 21, pp. 15-27, 2004.

Reham R. Mostafa was born in Abu Dhabi, UAE in 1983. She received her B.Sc., M.Sc., Ph.D degrees in information systems from Mansoura University, Egypt in 2005, 2009 and 2014, respectively. Currently she is an associate professor at Information Systems Department, Faculty of Computers and Information, Mansoura University, Egypt.

Hamdy K. Elminir was born in EI-Mahala, Egypt in 1968. He received the B.Sc. in Engineering from Monofia University, in 1991 and completed his master degree in automatic control system in 1996. He obtained his PhD degree from the Czech Technical University in Prague in 2001. Currently he is an associate professor in Faculty of Engineering, Kafr-Elshiekh University, Egypt.

Alaa El-Din Mohamed of Faculty of Computers and Information Systems, Mansoura University. Graduated in Mansoura University from electrical engineering department in 1982. Obtained Master degree in 1988 and Doctoral degree in 1992. Main research points currently are intelligent information systems and e-Learning.