DCT Based Digital Image Watermarking System

May Phone Myint, Thandar Win
University of Computer Studies (Mawlamyine), Myanmar
mayphonemyint88@gmail.com, thandarwin77@gmail.com

Abstract

Digital image watermarking is a method trying to embed small image inside a large original image. The original image will be converted into frequency domain to obtain the Discrete Cosine Transform (DCT) matrices from its block. DCT is mathematical tools, for embedding data into an image, to transform a signal from spatial to frequency domain. The logo image is embedded in random color components of the original image, as well as in random positions in each selected block. RC4, a pseudorandom bit generator, produces a stream of 8-bit numbers that are supposed to be truly random. The stream cannot be predicted without knowledge of the input key. RC4 is used to prevent from attackers when transferring watermark digital image pass over insecure network. After constructed the digital watermark image, send the image from sender side to receiver side. On the receiver side, accept the watermark image and extract the watermark image, by using IDCT and hidden logo image is received at the receiver side.

Keywords: Steganography, Digital Image Watermarking, DCT, RC4

1. Introduction

With the development of Internet technologies, digital media can be transmitted conveniently over the Internet. However, message transmissions over the Internet still have to face all kinds of security problems. Therefore, how to protect secret messages during transmission becomes an essential issue for the Internet. Encryption is a well-known procedure for secure data transmission. The commonly used encryption schemes include DES (Data Encryption Standard), AES (Advanced Encryption Standard) and RSA. These methods scramble the secret message so that it cannot be understood. Hence, a new scheme, called "steganography", arises to conceal the secret messages within some other ordinary media (i.e. images, music and video files) so that it cannot be observed. Two other technologies that are closely related to steganography are watermarking and fingerprinting.

Watermarking is a protecting technique which protects (claims) the owner's property right for digital media (i.e. images, music, video and software) by some hidden watermarks. Therefore, the goal of steganography is the secret messages while the goal of watermarking is the cover object itself. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels [1].

This paper is organized as follows: Section 2 focuses on the related work of the system. Section 3 presented the background theory of Discrete Cosine Transform and RC4. Section 4 explains design and implementation of the system and Section 5 is the results and discussion. Conclusions of this paper are described in Section 6.

2. Related Works

Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection.

The author S.P.Mohanty, University of South Florida [8] wrote about the Digital Watermarking of a tutorial review Tampa. S.Baba, L.Krikor, T.Arif and Z.Shaaban, Applied Science University, Jordan [6] researched about Watermarking of digital images in frequency domain. R.Munir, B.Riyanto, S. Sutikno and W.P.Agung, Bandung Institute of Technology, Indonesia [4] were written An asymmetric watermarking method in the DCT domain based on RC4-Permutation and chaotic map, The author S. Ali Khayam from the department of Electrical & Computer Engineering, Michigan State University[5] wrote the Discrete Cosine transform (DCT) theory and application,

In this paper a digital image watermarking system is developed by using DCT in frequency domain.

3. Background Theory

The use of techniques in the watermarking can be divided into various categories. They can be classified according to application, source type (image, video, audio, text), human perception, and technique used. In this system, **DCT** and **RC4** are

used for watermark embedding and extraction processes.

3.1 Digital Image Watermarking

Watermarking (data hiding) is the process of embedding data into a multimedia element such as an image, audio or video file. This embedded data can later be extracted from, or detected in, the multimedia for security purposes. In general, a digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity [6].

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows.

1. Image Watermarking
2. Video Watermarking
3. Audio Watermarking
4. Text Watermarking

Watermarking system consists of watermark embedder and watermark detector. The inputs to the watermark embedder are the watermark, the cover media data and the embedding security key.

During images transfer, data integrity is not really secure. Watermarking can be an answer to such problems. The watermarking objective is to embed visible or invisible message inside the image data, see Figure 1. Watermarking techniques can be divided into various categories in various ways.

The watermarks can be applied in **spatial domain**. An alternative to spatial domain watermarking is **frequency domain** watermarking. It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques [8].

Watermarking consists of three main stages: insertion, detection and the removal of a watermark. The detection and removal are usually considered together. An embedding algorithm is used to embed the watermark in the image. The extraction algorithm recovers the watermark, which requires the same secret key that was used for watermark embedding [6].

Watermarking applications include copyright protection, authentication, embedded and hidden information. Visible watermark is a secondary translucent overlaid into the primary image. The invisible watermark is embedding in such a way that an alternation made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism [8].

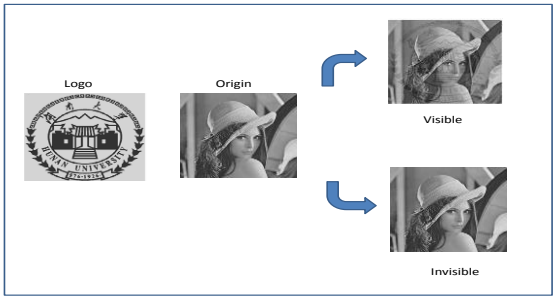

Figure 1: Visible and Invisible Methods of Watermarking System

Attacks on Watermark: According to the watermarking jargon, an *attack* is any processing that may mess up detection of the watermark or communication of the information provided by the watermark. The processed watermarked data is then called *attacked data*. Robustness against attacks is an important issue for watermarking schemes. The usefulness of an attacked data can be measured by its perceptual quality and the amount of watermark destruction can be measured by criteria such as miss probability, probability of bit error, or channel capacity. An attack may succeed in defeating a watermarking scheme if it distorts the watermark beyond tolerable limits while maintaining the perceptual quality of the attacked data. The wide class of existing attacks can be divided into four main groups: removal attacks, geometrical attacks, cryptographic attacks and protocol attacks.

Security on Watermark: In the implementation of watermarking system, the security over attack is an essential one. To have a better security, RC4 random key generation algorithm is applied in embedding the logo image processes. RC4 is a stream cipher and the random keys produced from this cannot be predicted without the knowledge of input secret key. Watermarking system is improved and can protect the malicious attackers who tried to get the hidden logo images by applying RC4 random key generation in this system.

3.2 DCT (Discrete Cosine Transform)

Many digital image and video compression schemes use a block-based DCT, because this algorithm minimizes the amount of data needed to recreate a digitized image. The original image is decomposed in 8×8 blocks; these blocks are transformed from the spatial to the frequency domain by the DCT [3]. Embedding the watermark into the transform-domain can increase the robustness, when the watermarked image is tested after having been subjected to common image processing [4].

The DCT allows an image to be divided into different frequency sub-bands: low frequency, middle frequency, and high frequency. Embedding the watermark into the low-frequency sub-bands coefficient can degrade the image quality, whereas high frequency components are easily discarded after low pass filtering. Therefore, for balancing the image fidelity and robustness, most watermarking techniques embed the watermark into the middle-frequency sub-bands coefficients [4]. The equations of forward and inverse DCT are-

Forward DCT:

$$F(u,v) = C(u)C(v)\left[\sum_{x=0}^{(N-1)}\sum_{y=0}^{(N-1)} f(x,y)\cos\frac{(2x+1)u\pi}{2N}\cos\frac{(2y+1)v\pi}{2N}\right]$$

Inverse DCT:

$$f(x,y) = \left[\sum_{u=0}^{(N-1)}\sum_{v=0}^{(N-1)} C(u)C(v)F(u,v)\cos\frac{(2x+1)u\pi}{2N}\cos\frac{(2y+1)v\pi}{2N}\right]$$

where: $C(u) = \frac{1}{\sqrt{N}}$, $C(v) = \frac{1}{\sqrt{N}}$ for u,v = 0;

$C(u) = \sqrt{\frac{2}{N}}$, $C(v) = \sqrt{\frac{2}{N}}$ for u,v = 1 through N-1;

N = 8 or 16

3.3 RC4

In the implementation of the system, RC4 is applied to generate the random key for embedding the images. Ron's Code #4 (RC4), is a variable-key-size stream cipher developed by Ron Rivest for RSA Data Security, Inc. RC4 like as a streaming cipher encrypts plaintext one byte at a time, but also can be designed to encrypt one bit a time or even units larger than a byte at a time. In this structure a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are supposed to be truly random, the pseudorandom stream can't be predicted without knowledge of the input key. The output of the generator is called a key stream. It is combined one byte a time with the plain text stream using the bitwise exclusive-OR (XOR) operation [6].

RC4 is simple to describe. It has an 8 * 8 S-box: S0, S1…, S255. The entries are a permutation of the numbers 0 through 255, and the permutation is a function of the variable-length key. It has two counters, i and j, initialized to zero [6]. To generate a random byte,

i := 0
j := 0
while Generating Output:
i := (i + 1) mod 256
j := (j + S[i]) mod 256
swap (&S[i],&S[j])
output K=S[(S[i]+S[j])mod 256]
endwhile

The most important aspect of RC4 is the security it offers. It should also not be feasible to determine the key (seed) from knowledge of any generated values. In particular, the output must be unpredictable in the absence of knowledge of the inputs. If the key (seed) is unknown, the next output number in the sequence should be unpredictable in spite of any knowledge of previous random numbers in the sequence. This property is known as forward unpredictability.

4. Design and Implementation of the System

The system has implemented digital image watermarking system to prevent information from access by unauthorized parties. The proposed method based on the idea of decomposing the image into 8x8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT. Then, RC4 generated 8 bits numbers that are applied on logo image with XOR operation. Logo image is used to embed in the cover media (original image). The result of the output is a watermark image, which is not differing from the original image in features.

4.1 System Design

In this system, there are two sides (sender and receiver). Sender side produces watermark image, encrypt with DCT and RC4 for security purposes. The watermark image is then sent to the receiver. In the receiver side, firstly need to accept the watermark image and decrypt with inversed discrete cosine transform (IDCT) and RC4. Figure 2 shows overview of the system design.

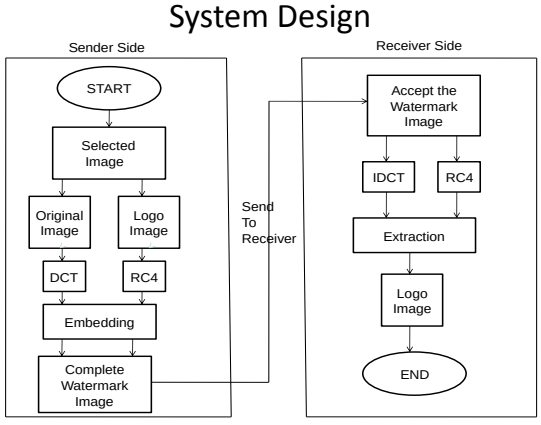

Figure 2: Overview of the System Design

4.1.1 Sender Side

In digital image watermarking system, it needs two types of images: an original image (source

image) and a logo image (watermark image). Sender side selects original image and decomposed into 8x8 blocks. And then apply DCT mathematical calculations on each block. That takes a signal and transforms it from spatial domain into frequency domain.

The secret key is put in the extraction step where RC4 generates 8 bits stream random numbers. This stream is transformed in logo image with XOR operation. This step makes plain image (logo) to cipher image. Cipher logo image is embedded on original image by applying DCT. After embedding the image, a complete watermark image is accomplished from the sender side. Figure 3 shows the process of sender side in the watermarking system.

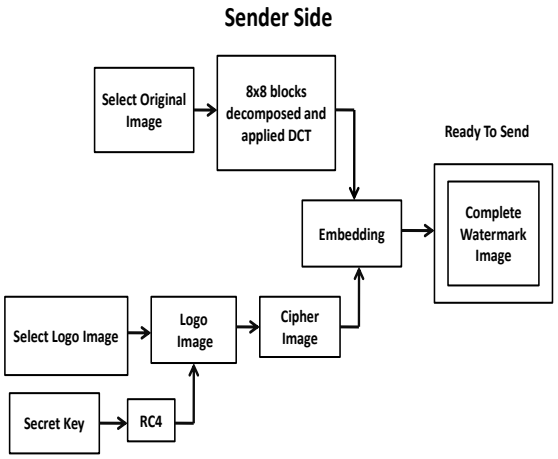

Figure 3: Sender Side of Watermarking System

4.1.2. Receiver Side

On the receiver side, the watermark image is accepted from sender. After getting the watermark image, applies IDCT and symmetric secret key RC4 to extract the embedded logo image. If the secret key is unknown, or false the recipient does not produce logo image. The same symmetric key is used in both sender and receiver side. The secret key is used in the decryption process, and finally the logo image is generated at the receiver side. The process for the receiver side is as shown in Figure 4.

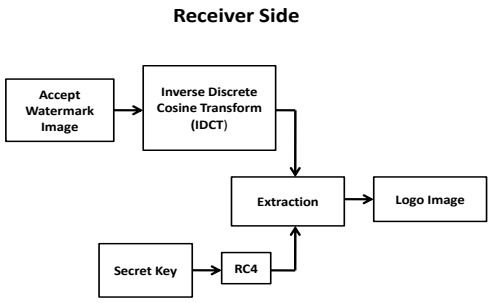

Figure 4: Receiver Side

4.2 Implementation of the System

This "DCT Based Digital Image Watermarking System" has been implemented using Visual C#.Net Programming language. The original image, that is enable to hide the selected logo image. This experiment used original image size of (1024x768) in Figure 5 and a logo of size of (112x138) in Figure 6. In this system, there are two sides: sender side and receiver side.

Figure 5: Original Image (Blue Whale) Size 1024x768

Figure 6: Watermark Logo Image of Size 112x138

4.2.1 Sender Side

In the sender side, select the original image (cover image) and logo image (watermark image). The logo image is smaller than original image. Then the original image is applied by DCT to transform spatial domain to frequency domain. Also the logo image is encrypted with secret key using RC4. After these steps, the logo image is embedded into the original image. In the end of the system, a complete watermark image is produced and that is ready to send to the receiver. Figure 7 displays the logo image decryption with secret key. In this experiment, the secret key "bluewhale" is used. Figure 8 described encrypting process of the watermarking system.

Figure 7: Logo Image Encryption with Secret Key

Figure 8: Embed Logo Image into Original Image

4.2.2 Receiver Side

In receiver side, need to receipt watermark image from sender side and extract the logo image. For extracting process, transform IDCT and RC4 needs the secret key. This key is the same, both sender and receiver sides. Figure 9 shows encrypting with false secret key and Figure 10 is true secret key "bluewhale".

Figure 9: Decrypt with False Secret Key

Figure 10: Decrypt with True Secret Key

5. Results and Discussion

In the DCT based digital image watermarking system, the original image and logo image are embedded and extracted by using DCT and RC4 functions. Secret key is used for security purposed. By using the random key in this system, it is not feasible to get the embedded logo image from malicious attackers. RC4 generates pseudorandom bits which are used as secret key for the embedding process that provides an advantage for protecting attacks from others. In the Watermarking system, the logo image is embedded into original image. The output of the watermark image is nearly the same as original image in human perception. This is the advantage of the system in the insecure channel where the attackers would not find the embedded image easily and so the hidden images are safely transferred to others. In case the attacker knows the logo is embedded, it cannot be broken, without the knowledge of the secret key. Details of the implementation are described in Figure 7, 8, 9 and 10 of the Section 4.

6. Conclusions

Digital image watermarking is important to all kinds of media. In this paper, digital image watermarking system is implemented by using Discrete Cosine transformation in frequency domain and RC4 algorithm. In the proposed method, the embedding process is hidden under the transformation i.e. DCT and inverse DCT. These operations are encoding of secret image keep the images away from stealing, destroying from unintended users and hence the proposed method may be more robust against attack. Hence RC4 can work as a security solution for them, with a very fast performance and strong degree of security. Therefore, using the DCT and RC4 with secret key provide the watermarking system to achieve authentication for establishing identity of sender and receiver.

References

[1] A.Nag, S. Biswas, D.Sarkar, P.P. Sarkar,"*A novel technique for image steganography based on Block-DCT and Huffman Encoding",* University of Kalyani, Nadia –West Bengal, India.

[2] A.M.Riad, A.R.Shehata, E.K.Hamdy, M.H. Abou-Alsouad, T.R.Ibrahim, "*EVALUATION OF THE RC4 ALGORITHM AS A SOLUTION FOR CONVERGED NETWORKS*", Journal of ELECTRICAL ENGINEERING,VOL.60, NO.3, 2009.

[3] L.Krikor, S.Baba, T.Arif, Z.Shaaban**,"***Image Encryption Using DCT and Stream Cipher***",** ***http://www.eurojournals.com/ejsr.htm.***

[4] R.Munir, B.Riyanto, S.Sutikno & W.P. Agung, "*An Asymmetric Watermarking Method in the DCT Domain Based on RC4-Permutation and Chaotic Map",* Bandung Institute of Technology, Indonesia.

[5] S.A.Khayam, "The Discrete Cosine Transform (DCT): Theory and Application", Department of Electrical & Computer Engineering, Michigan State University.

[6] S.Baba, L.Krikor, T.Arif and Z.Shaaban , "*Watermarking of digital images in Frequency Domain*", Faculty of information Technology, Applied Science University, Jordan.

[7] S.M. Rafizul Haque, "*Singular Value Decomposition and Discrete Cosine Transform Based Image Watermarking*".

[8] Saraju P. Mohanty .Dept of Comp Sc and Eng, "*Digital Watermarking: A Tutorial Review*", University of South Florida Tampa.