Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.859 – 864

RESEARCH ARTICLE

Effective Copyright Protection of Digital Products by Embedding Watermarking

Monika Craig [1], Prof. Deepak Kapgate[2]

[1]Department of CSE G.H. Raisoni Academy of Engineering and Technology, Nagpur University Maharashtra India
[2]Department of CSE G.H. Raisoni Academy of Engineering and Technology, Nagpur University Maharashtra India

[1] monika.craig289@gmail.com, [2] deepak.kapgate@raisoni.net

---

Abstract - The watermarking of digital images, audio, video and multimedia products in general have been proposed for resolving copyright ownership and verifying originality of content .This paper studies the contribution of watermarking for developing the protection schemes. Wolfgang and Delp Algorithm (Technique) is used in case of watermark Embedding. The algorithm proposed the scheme of watermarking by encrypting the watermark image using symmetric encryption like DES. According to the method, the watermark symbol to be encrypted first using DES and then embedding it into RGB vectors of original image using SVD transformation sampling. The experiment proves that the algorithm of embedding watermark has better robustness to JPEG compression attack.

Keywords –Digital watermarking; copyright protection; SVD (singular value decomposition); DES; Watermark embedding algorithm; watermark extraction process

---

I. INTRODUCTION

The rapid expansion of the Internet and the overall development of digital technologies in the past years have sharply increased the availability of digital multimedia content. One of the great advantages of digital data is that it can be reproduced without loss of quality. However, it can also be modified easily. In many contexts, such for legal evidence and for video security systems, any modifications of image, video or audio data have to be detected. Therefore, some work needs to be done in order to develop security systems to protect the information contained in digital data (Cox, 1997). Watermarking (Chiou, 1999; Cox, 2002; Cox, 2001; Nikolaidis, 1996; Wolfgang,1996; Wolfgang, 1999) is the process of embedding data into a multimedia element such as an image, audio or video file. Digital watermarking is applied for copyright protection, content authentication, detection of illegal duplication and alteration, feature tagging and secret communication[1,3,4,5]. Digital watermarking is the hiding of a secret message or information within an ordinary message and its extraction at its destination. The secret message is the digital watermark. An

effective watermarking scheme must successfully deal with the triple requirements of imperceptibility, robustness and capacity [11], [12]. This embedded data can later be extracted from, or detected in, the multimedia for security purposes. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction, or detection, algorithm. Watermarks can be embedded in the pixel domain or a transform domain. The most important uses of watermarks include copyright protection and ownership authentication for the multimedia data that flourish at the advent of the Internet (Chang, 2002; Nikolaidis, 1996; Petitcolas, 2000). Identification of the origin of content requires the embedding of a single watermark into the content at the source of distribution. To trace illegal copies, a unique watermark is needed based on the location or identity of the recipient in the multimedia network.

A. *Basic concepts of digital watermarking technology*

The digital watermarking algorithm contains two basic aspects: the watermark embedding and the watermark extraction or detection in [1].The watermark can be made up of various models, for example random number sequence, digital identifier , text and image and so on. From a consideration of the robustness and security, we generally need to encrypt for the watermark image.

Watermark embedding process: We suppose the algorithm E, original image I and watermark image W is exist, and then the watermark image I_w can be expressed as follows:

$$I_w = E(I, W) \quad (1)$$

The watermark embedding process is shown in Fig.1.

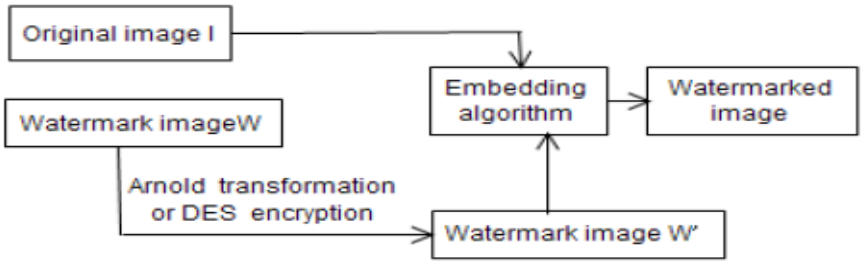

Figure 1.The watermark embedding process

Watermark detection process: watermark detection is the most important step in the watermarking algorithm. If the detection process is defined as the decoding function D, the output can contain a variety of information data stream, such as text and image, etc. And the detection process also uses 0 and 1 to determine whether watermark is present or not for decision-making and judgment. If the original image is I and the image with the problem of copyright is I_w, then

$$W' = D(Iw, I) \quad (2)$$

Otherwise:

$$C(W'', W^*, K, \$) = \begin{cases} 1 & W'' \text{ exists} \\ 0 & W'' \text{ Doesn't exist} \end{cases} \quad (3)$$

Where W^* is the extracted watermark image, K is the password, the function C is to do the related testing, and $\$$ is the decision threshold. A detection function of the formula (3) is the easiest one of ways to create an effective watermark framework, such as similarity of hypothesis or watermark test. The watermark detection process is shown in Fig.2.

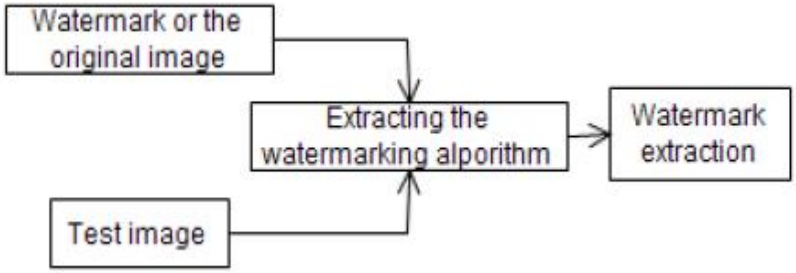

Figure 2. The watermark detection process

II. AN ALGORITHM OF COLOR IMAGE WATERMARK BASED ON SVD TRANSFORMATION

A. Scrambling Encryption of watermark Image

1) DES Encryption

Data Encryption Standard (DES) is a data encryption algorithm proposed by W. Tuchman, C. Meyers etc. It is used for non-critical information encryption of commercial and government by U. S. National Bureau of Standards. DES is a typical symmetrical cryptosystem, its encryption key and deciphers are the same. The fast speed of encryption and decryption, easy to implement of the algorithm is and security is the most important advantage of DES. The basic idea of the DES algorithm is that plaintext every 64 bits is divided into a group under the control of a 64-bit key, and then to encryption according to group in [1]. The specific framework is shown in Fig.3.

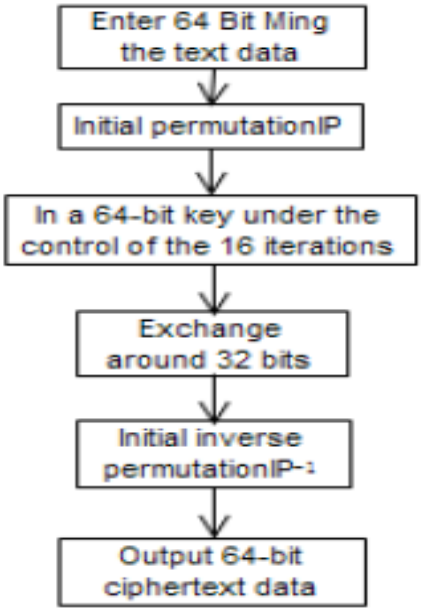

Figure.3 The Basic framework of DES encryption

B. Singular Value Decomposition(SVD): Singular Value Decomposition(SVD) is a numerical technique for diagonalizing matrices in which the transformed domain consists of basis states that is optimal in some sense. The SVD of an N x N matrix A is defined by the operation:

$$\boldsymbol{A = U\,S\,V^{T}} \tag{4}$$

Where $\boldsymbol{U}$ and $\boldsymbol{V} \in \boldsymbol{R\ N\ x\ N}$ are unitary and $\boldsymbol{S} \in \boldsymbol{R\ N\ x\ N}$ is a diagonal matrix. The diagonal entries of $\boldsymbol{S}$ are called the singular values of A and are assumed to be arranged in decreasing order $\boldsymbol{\sigma i > \sigma i + 1}$. The columns of the $\boldsymbol{U}$ matrix are called the left singular vectors

while the columns of the V matrix are called the right singular vectors of ***A.*** Each singular value ***σi*** specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer. In SVD-based watermarking, a frame image is treated as a matrix decomposed into the three matrices;***S, U*** and ***V T,*** as shown below.

$$\text{Svd}(A) = \begin{bmatrix} U_{1,1} & . & . & U_{1,n} \\ U_{2,1} & . & . & U_{2,n} \\ . & . & . & . \\ U_{n,1} & . & . & U_{n,n} \end{bmatrix} \begin{bmatrix} S_{1,1} & 0 & 0 & 0 \\ 0 & S_{2,2} & 0 & 0 \\ . & . & . & . \\ 0 & 0 & 0 & S_{n,n} \end{bmatrix} \begin{bmatrix} V_{1,1} & . & . & V_{1,n} \\ V_{2,1} & . & . & V_{2,n} \\ . & . & . & . \\ Vn,1 & . & . & Vn,n \end{bmatrix}$$

1) SVD-Based Video Watermarking Algorithm

The algorithm is based on transforming the host video using the SVD operator and then embedding the watermark information in the S, U, or V matrices diagonal-wise. The proposed algorithm , the first embeds the watermark into the original video clip, while the other extracts it form the watermarked version of the video clip. A block diagram showing the embedding and extraction procedure of the algorithm is shown in Figure 4.

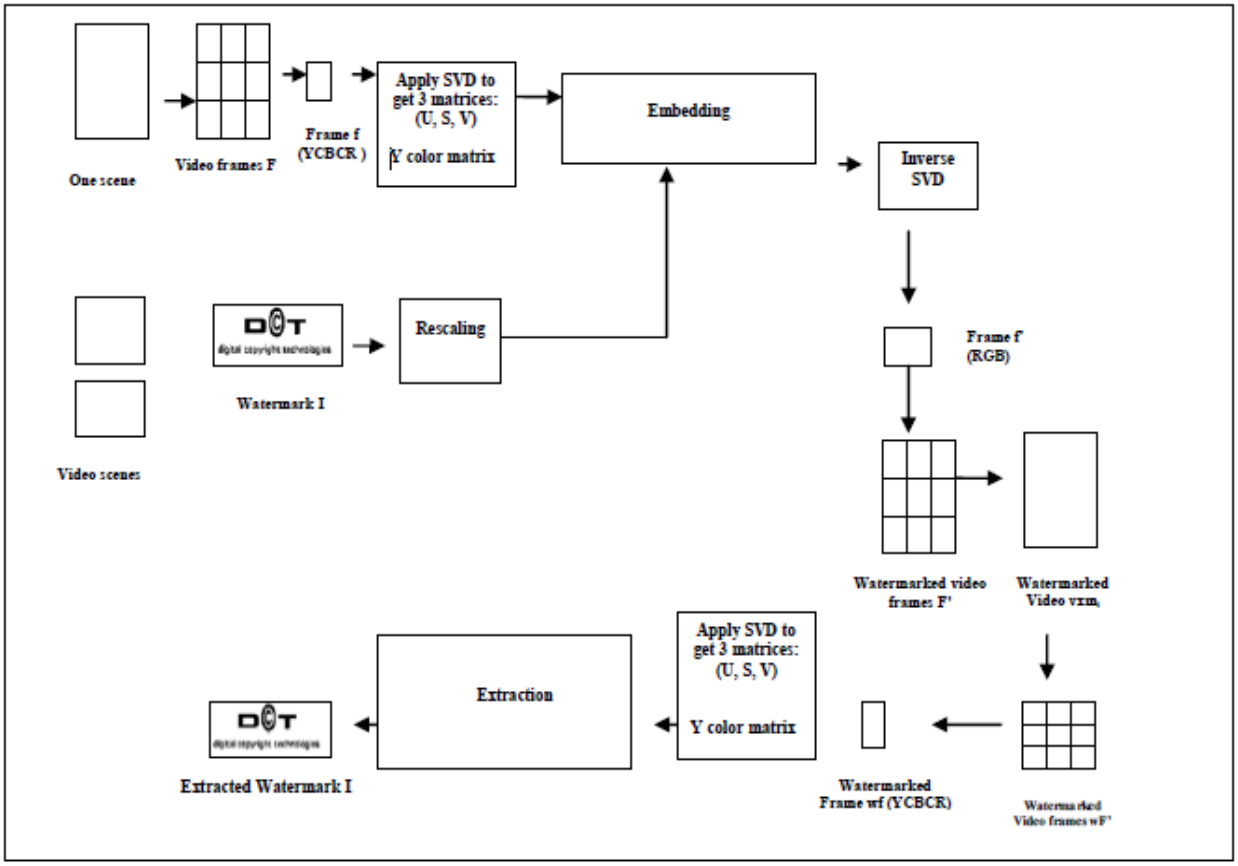

Figure 4.Block diagram of watermark embedding and extraction procedure

Watermark Embedding Procedure

Step 1:The watermark image which is to be embedded with the video is srambled by using DES encryption.
Step 3: Process the frames of each video scene using SVD.
Step 4: Convert every video frame *F* from RGB to BGR color matrix format.
Step 5: Compute the SVD for the Y matrix in each frame *F*. This operation generates 3Matrices (U,S,V) such as:

$$Y = U_Y S_Y V_Y \quad (5)$$

Step 6: Rescale the watermark image so that the size, of the watermark will match the size of the matrix which will be used for embedding either U, V or S.
Step 7: Embedding can be done in one of the three SVD matrices: *U, V, or S*.
Step 8: Apply inverse SVD on the modified coefficient matrix S '. such as:

$$Y' = U_Y S_{Y'} V_Y^T \quad (6)$$

Where Y' is the updated luminance in the BGR color representation. This operation produces the final watermarked Video frame *F*'.
Step 9: Convert the video frames *F'* from BGR to RGB color matrix.
Step 10: Reconstruct frames into the final watermarked Video scene *Vsi'*.
Step 11: Reconstruct watermarked scenes to get the final watermarked Video clip.

Watermark Extraction Procedure

The watermark extraction is the inverse process of watermark embedding. The algorithm steps are as follows:
Step 1: Divide the watermarked Video clip *V* ' into watermarked scenes *Vsi'*.
Step 2: Process the watermarked frames of each watermarked video scene using SVD.
Step 3: Convert the video frame ***F'*** from RGB color matrix to BGR.
Step 4: Compute the SVD for the Y matrix in frame *F'*. , this operation generates 3 Matrices (U, S, V).
Step 5: Extraction is done in one of the three SVD matrices: *U, V, or S*, as follows:
Step 6: Decrypting the watermark image by DES.
Step 7: Construct the image watermark *WVsi* by cascading all watermark bits extracted from all frames.
Step 8**:** Repeat the same procedure for all video scenes.

III. RESULT AND DISCUSSION

We Programed With java to realize the algorithm above and did watermark signal embedding and detecting using color video as original carrier and image as watermark. Fig. 5 is the scene1 of video and image of watermark information.Fig.6 is the watermark video that contain invisible watermark image.Fig.7 is the watermark video that contain visible watermark.

Figure 5.scene1 of video and Image of watermark

Figure 6. Invisible watermark

Figure 7. Visible watermark

We are performing analysis based on 3 parameters such as Gaussian noise attack, Shearing attack, JPEG Compression attack on which digital watermarking should react

PSNR = lO\OglO[255^2/MSE]

MSE = Mean square error –Sum[sum(error * error)]/(M*N)

TABLE 1.Analysis Performance of Attacks

Video Scenes	Gaussian noise attack	Shearing attack	JPEG Compression attack
Scene1	23.48	23.11	22.01
Scene 2	22.11	21.09	20
Scene 3	24.12	23.99	22.05

IV. CONCLUSION

In this paper, SVD-based digital video watermarking algorithm were proposed. In the algorithm, watermarking information was embedded in the diagonal elements of S, U, or V matrices. The algorithm encrypts the binary watermark image by DES which is embedded in the RGB channels decomposed by video. The watermark embedding has no influence to the original video, there is almost no difference between the watermark image extracted from the image containing watermark and the original watermark video. However, embedding in the diagonal elements of matrix produced higher robustness values against JPEG attack.

REFERENCES

[1] Yong Zhu, Xiaohong Yu, Xiaohuan Liu, *"An Image Authentication Technology Based on Digital Watermarking"* International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS) 2013 IEEE.

[2] A. V. Subramanyam, Sabu Emmanuel, *Member, IEEE*, and Mohan S. Kankanhalli, *Senior Member, IEEE,"* Robust Watermarking of Compressed and Encrypted JPEG2000 Images*"* IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 14, NO. 3, JUNE 2012.

[3]B. Sridhar ,Dr.C.Arun *"On Secure Multiple Image Watermarking Techniques using DWT"* 2012 IEEE.

[4] Ying Zhang, Jiqin Wang, Xuebo Chen *"Watermarking Technique Based On Wavelet Transform For Color Images"* 2012 IEEE.

[5] Qing Liu, Jun Ying *"Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis"* 2012 IEEE.

[6] Manish K Thakur, Vikas Saxena, J. P. Gupta," A Performance Analysis of Objective Video Quality Metrics for Digital Video Watermarking" 978-1-4244-5540-9/10/$26.00 ©20 1 0 IEEE.

[7] Yasunori Ishikawa, Kazutake Uehira, and Kazuhisa Yanaka, "Optimization of Size of Pixel Blocks for Orthogonal Transform in Optical Watermarking Technique" JOURNAL OF DISPLAY TECHNOLOGY, VOL. 8, NO. 9, SEPTEMBER 2012,IEEE.

[8] Abdul R. Zubair, *Member, IEEE*, Olasebikan A. Fakolujo, *Member, IEEE* and Periasamy K. Rajan,
Fellow, IEEE," digital watermarking of still images with color digital watermarks*"* 978-1-4244-3861-7/09/$25.00 ©2009 IEEE

[9] Satyendra N. Biswas.et al.," MPEG-2 digital video watermarking technique" 978-1-4577-1772-7/12/$26.00 ©2012 IEEE.

[10] F. Liu C.-K. Wu," Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners", IET Inf. Secur., 2011, Vol. 5, Iss. 2, pp. 121–128.

[11] Fei C., Kundur D., and Kwong R.H. "Analysis and Design of secure watermark-based authentication Systems", IEEE Trans. on Information Forensics and Security 1 (1) (2006). p. 43-55.

[12] Abdul R. Zubair et al.*,"* digital watermarking of still images with color digital watermarks", 978-1-4244-3861-7/09/$25.00 ©2009 IEEE.

