

# A Novel Scheme for Digital Rights Management of Images Using Biometrics

**N.Nagamalleswara Rao**

Professor & HOD Department of CSE  
Chebrolu Engineering College, Chebrolu  
Andhra Pradesh, India

**Prof. P. Thrimurthy**

HOD, Department of CSE  
Nagarjuna university  
Guntur, Andhra Pradesh  
India

**Dr. B. Raveendra Babu**

HOD, Department of CSE  
RVR &JC College of Engineering  
Guntur, Andhra Pradesh  
India

## Summary

The enormous development in digital technologies has necessitated the owners to pay great attention in protecting their digital contents. Recently, watermarking has been employed by researchers for the protection of digital documents. However the embedded watermark data can be easily hacked by the hackers and thus result as a threat to protection of digital content. In this paper, we have developed a novel scheme for protecting the copyrights of digital images by utilizing both biometrics and digital watermarking. In our scheme, the fingerprint biometric feature of the owner is used to generate the watermark. The minutiae points are extracted from the fingerprint and the coordinates of the minutiae points are represented as a matrix and are eventually utilized as watermark. The embedding and extraction of watermark is performed in the DCT-SVD domain. In case of any ownership dispute on the image, the watermark i.e., the coordinates of the minutiae points, is extracted from the watermarked image and compared against the coordinates of minutiae points extracted from the fingerprint of the person claiming ownership. If they match, the claiming person is the actual owner of the image. Thus the biometric feature utilized in our scheme ascertains the information to be very secure. Besides there is no necessity to carry the information and it cannot be hacked by the hackers as well.

## Keywords:

*Biometrics, Digital Watermarking, Digital Rights Management (DRM), Copyright protection, Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), Fingerprint, Minutiae Points.*

## 1. Introduction

The security of intellectual property has always been a concern and no perfect solution has been developed so far. The problem is considered even complicated in the digital world due to the fact that the copying data is being done easily and quickly. The presence of internet has also facilitated the rapid and effortless distribution of the files and information. This along with the intricacy of tracking distributors of the illegal content has lead to the omnipresence of illegal file sharing. This necessitated the need for managing the rights of digital content. Digital Rights Management (DRM) refers to a range of access control technologies used to limit or restrict usage of digital content. The Digital Rights Management (DRM)

technologies intend to enhance the kinds and/or scope of control that rights-holders can affirm over their intellectual property assets [28]. DRM refers to the protection of intellectual property rights for multimedia content. These days, the distribution of digital music, images, video, books and games over the internet to the end-users has become quite easy owing to the extensive utilization of internet and the enhancements in streaming media and compression technology. The protection and restricted circulation of the expensive digital assets can be facilitated through Digital Rights Management systems [37].

Digital Rights Management solutions assist the protection of confidential information and premium content from unauthorized use even by authorized users in the corporate and government sectors [12]. The most vital function of DRM system is the copyright protection. The copy restriction such as permitting no or one or several unlimited copies of the multimedia data, and with or without rights to produce copies of these copies can be enforced by the DRM system. [3]. Thus the use of digital watermarking techniques that embed information recognizing the copyright owner's identity within the content is regarded as a promising copyright protection technique [15]. DRM consists of certain techniques which includes encryption, copy control, digital watermarking, fingerprinting, traitor tracing, authentication, integrity checking, access control, tamper-resistant hard- and software, key management and revocations as well as risk management architectures [29].

The growing research area, Digital watermarking, has its roots in computer science, cryptography, signal processing, Image Processing and communications [10]. The primary objective of digital watermarking is to embed small amount of secret information, i.e., the watermark into the host digital productions like the image and audio, thus facilitating the extraction at a later stage for the purposes of copyright assertion, authentication, and content integrity verification and the like [11]. Owing to the good results that were obtained, watermarking methodologies have attracted attention [7, 8, 9]. Digital watermarking techniques can be utilized to protect the intellectual property rights of the data by embedding the proprietary

information, such as password and company logo, in the host data [3], [13]. The determination of ownership and the detection of tampering are the two purposes of watermarks [17]. The Digital watermarks of ownership are embedded onto digital content for copyright protection, ownership affirmation, and integrity checks since digital content can be employed to obtain the verification of copyright violation after an attack [4]. The techniques like watermarking assist in controlling the unauthorized replication or exploitation of digital content [4], [13], [14].

Although watermarking is used in many applications, still there is a threat to security for the embedded watermark against possible malicious attacks. Digital watermarking embeds some information regarding the ownership into the digital data, hence guaranteeing copyright protection. Intended for variety of purposes like copyright protection, access control, and broadcast monitoring, the extraction of the embedded data in the future is possible [5]. The information about ownership can be any privacy information that exclusively identifies the owner during ownership controversies, such as password, logo or the like. The aforesaid information can possibly be hacked by the hackers. There is a possibility of the owner losing or forgetting the same as well. The hackers may at times brute-force the information and claim the ownership ultimately. In addition, the solution for the problem of rightful ownership has not been properly solved. Therefore the design of DRM system needs to address the above mentioned security issues and also solve the ownership dispute.

In this paper, we have focused on the prevention of disputes that arise out of ownership claims on digital images and a novel and efficient scheme to deal with it has been developed. In the proposed scheme, we utilize both watermarking and biometrics to protect the digital contents. The main intention of utilizing biometrics is due to some of its characteristics namely security and confidentiality. Biometrics is a radically emergent technology that is extensively applied in forensics like the criminal identification and prison security and probably employed by a wide diversity of application areas. In future, biometrics will play a vital role in security [1]. Ultimately if any ownership dispute arises, biometrics helps to solve the situation because of the insertion of biometric feature as the watermark. In the proposed scheme, the minutiae points are extracted from the fingerprint of the owner. Then the coordinates i.e., the location of the minutiae points are determined and represented as a matrix. The singular values of this matrix are calculated and used as the watermark in the proposed scheme. The watermark embedding and extraction is performed in DCT-SVD domain using the method proposed by Alexander et al. [30] with modifications to a certain extent so as to cater our requirement. In case of any ownership dispute on the

image, the watermark is extracted i.e., the singular values of the coordinates of the minutiae points, from the watermarked image are extracted and compared against the singular values of the coordinates of minutiae points extracted from the finger print of the person claiming ownership. If both are similar, then we can conclude that the person claiming ownership is the actual owner of the image.

The paper is organized as follows; Section 2 presents a brief review of some of the works available in the literature that combines biometrics and watermarking for managing the rights of digital documents. In Section 3 the proposed novel scheme for digital rights management of images using biometrics is presented in detail. Section 4 describes the results of our experiments. Conclusions are summed up in Section 5.

## 2. Related Works

Our work is inspired by a number of previous works related to copyright protection of digital documents using digital watermarking and biometrics. Such works are reviewed below:

Justin Picard et al. [20] have presented a virtually fraud-proof ID document that works on a merger of three different data hiding technologies: digital watermarking, 2-D bar codes, and Copy Detection Pattern to be precise along with additional biometric protection. They have illustrated that the combination of data hiding technologies guards the document from any kind of forgery, in principle without any requirement for additional security features

Minerva M. Yeung et al [21], focused on the study of watermarking on images employed in the automatic personal identification technology based fingerprints. They investigated the effects of watermarking fingerprint images on the identification and extraction accuracy with the aid of invisible fragile watermarking technique for image verification applications on a particular fingerprint recognition system.

A methodology for the recognition of fingerprints with the aid of Artificial Neural networks was proposed by Mohamed Mostafa Abd Allah [22]. A clustering algorithm was employed by them for the identification of similar feature groups from template images generated from the same finger and a cluster core set was created. Their proposed feature extraction scheme was based on the diminution of information contents to the required minimum besides defining a certain part of the image as crucial in order to be omitted.

A user identification technique at H.264 streaming utilizing watermarking with fingerprints was presented by

Sooyeon Jung et al. [23]. The algorithm proposed by them consists of enhancement of a fingerprint image, watermark insertion using discrete wavelet transform and extraction after restoring. Their algorithm was capable of achieving robust watermark extraction against H.264 compressed videos.

A multimedia content protection scheme that worked on biometric data of the users and a layered encryption/decryption scheme were presented by Umut Uludag et al. Password-only encryption schemes are frequently prone to illegitimate exchange issues. The fraudulent usage of protected content can be reduced with the aid of biometric data along in association with hardware identifiers as keys. A combination of symmetric and asymmetric key systems was utilized by them for this purpose [24].

Mina Deng, et al., [25] have proposed a model for privacy infrastructures intended towards the distribution channel such that as soon as the picture is publicly available, the exposed individual gets an opportunity to find it and take appropriate action without any delay. Digital rights management techniques were applied in their proposed infrastructure, and data identification techniques like the digital watermarking and robust perceptual hashing were as well proposed to improve the distributed content identification.

A remote multimodal biometric authentication framework that worked on basis of fragile watermarking for the transmission of multi-biometrics over networks to server for authentication was proposed by Tuan Hoang, et al. [26]. Their proposed framework improves security and brings down bandwidth. Besides they also proposed a technique to compute bit priority level in a bit sequence denoting the numerical information to be embedded and merge with the existing amplitude modulation watermarking method.

Two distinct methodologies for the protection of on-line signature biometric templates were proposed by Emanuele Maiorana, et al., [27]. The first one deals with the utilization of cryptographic techniques to guard signature features, making it impossible to obtain the original biometrics from the stored templates. The second technique deals with the utilization of data hiding techniques for the design of a security scalable authentication system embedding some dynamic signature characteristics into a fixed depiction of the signature itself.

### 3. Novel Scheme for Digital Rights Management of Images Using Biometrics

A novel scheme for the digital rights management of images with the aid of biometrics has been presented in our research. The proposed work makes use of watermarking for managing the digital rights and ownership of images. The watermark data generated from the biometric feature of the owner is embedded into the original image. Owing to the fact that the fingerprint is the most reasonable and the most extensively utilized biometric feature, we have utilized the fingerprint of the owner in our scheme. Initially, the minutiae points are extracted from the fingerprint image. Then the locations i.e., the coordinates of the minutiae points are determined and its singular values are calculated using Singular Value Decomposition (SVD). These singular values are embedded into the original image using DCT-SVD domain image watermarking proposed by Alexander et al. [30]. In case of any claim of ownership on the image, the embedded singular values of the coordinates of minutiae points are extracted from the watermarked image and compared against the singular values of coordinates of fingerprint minutiae of the person claiming. This comparison will solve the ownership disputes i.e.) if the comparison becomes successful, the person claiming is the actual owner of the image.

#### 3.1. Fingerprint Minutiae Point Extraction

The extraction of minutiae points from the fingerprint image is presented in this sub-section. The fingerprint of an individual is distinct and does not change over the lifetime. An impression of the pattern of the ridges present in the finger creates a fingerprint. An individual curved segment is referred to as a ridge and the area amidst two adjacent ridges is known as a valley. Hence, the distinctiveness of the local ridge features and their associations define a fingerprint [32]. Local ridge features that appear either at a ridge ending or a ridge bifurcation are called Minutiae points. A ridge ending is formed out of the abrupt ending of a ridge. Ridge bifurcation is a point where the ridge splits into two or more branches [36]. The extraction of minutiae points from the fingerprint image involves three major steps:

- (i) Preprocessing
- (ii) Determination of Region of Interest (ROI)
- (iii) Minutiae points extraction

##### 3.1.1 Preprocessing

The fingerprint image is preprocessed before extracting minutiae points. The preprocessing step enhances the fingerprint image and involves the following: histogram equalization, image enhancement and binarization. They are described as follows:

**Histogram Equalization:** In general, the local contrast of many images is increased by this method, especially when the close contrast values of the usable data are used to represent the usable data of the image. The intensities can be better distributed on the histogram owing to this adjustment. The histogram equalization permits pixel value to expand the distribution of an image to increase the perceptual information of the image. The original histogram of a fingerprint image has the bimodal type. After the histogram equalization, the histogram obtained covers all the ranges from 0 to 255 and there is an improvement in the visualization effect [31].



Fig. 1. Original and Histogram Equalized Fingerprint Image

**Image Enhancement:** An enhancement process that improves the clarity of the ridge structures is essential owing to the fact that the ridge structures in fingerprint images are not always well defined. [35]. Image enhancement techniques are usually employed prior to minutiae extraction to obtain a more consistent estimation of minutiae locations. Also image enhancement techniques are frequently used to decrease the noise and improve the definition of ridges against valleys. In our work, for enhancing the fingerprint image, Fast Fourier Transform (FFT) is applied separately to each block of the image.

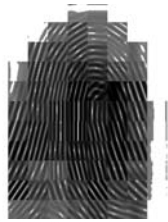


Fig. 2. Enhanced Fingerprint Image

**Binarization:** This process converts the enhanced image into binary image. During this step, a particular threshold is set, and the pixel values above this threshold are assigned to 1 and pixel values below the threshold are assigned to 0. Once the above mentioned process is carried out, the values in the binary image will be either 0 or 1. In our work, the adaptive threshold is chosen to be applied for the binarization process. In adaptive thresholding, the threshold for binarization is automatically set depending upon the fingerprint image.



Fig. 3. Binarized Fingerprint image

### 3.1.2 Determination of ROI (Region of Interest)

In this step, the ROI of the fingerprint image is determined. ROI is the region consisting of beneficial information. The fingerprint image area without effective ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area is sketched out since the minutiae in the bounded region are confusing with those spurious minutiae that are generated when the ridges are out of the sensor [32].



Fig. 4. Determined ROI of the Fingerprint Image

### 3.1.3. Minutiae Points Extraction

After determining the ROI, binary morphological operators are applied on the binarized fingerprint image. These operators are applied mainly for the purpose of removing any of the obstacles and noise from the image. The morphological operators applied in the following manner:

**Clean Operator:** Clean operator is applied to clean distortions occurring in the image. It removes isolated pixels i.e., individual 1's that are surrounded by 0's. For example, the centre pixel in this pattern is removed.



**Hbreak operator:** The Hbreak operator removes H-connected pixels. For example,



**Spur Operator:** The Spur operator is used to remove spur pixels. For example,

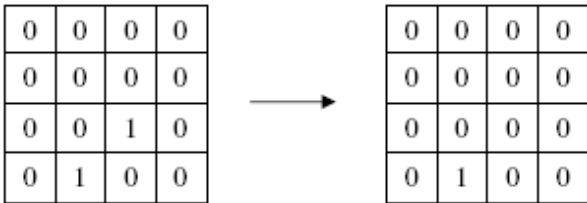


Fig. 5. Fingerprint Image after performing the morphological operations

A morphological operation that efficiently erodes away the foreground pixels till they become one pixel wide is called Thinning. As a result of the process, the thickness of each line of pattern in minimized to a single pixel width [34]. Ridge thinning aids in the removal of redundant pixels till the ridges become one pixel wide. The authors of [33] make use of the Ridge thinning algorithm the one that is utilized for Minutiae points' extraction in our technique. The image is parted into two different subfields resembling a checkerboard pattern. In the first sub iteration, pixel p from the first subfield is deleted only when all three conditions, G1, G2, and G3 are fulfilled. In the second sub iteration, pixel p from the first subfield is deleted only when all three conditions, G1, G2, and G3' are fulfilled

**Condition G1:**

$$X_H(P) = 1$$

Where

$$X_H(P) = \sum_{i=1}^4 b_i$$

$$b_i = \left\{ \begin{array}{l} 1 \text{ if } x_{2i-1} = 0 \text{ and } (x_{2i} = 1 \text{ or } x_{2i+1} = 1) \\ 0 \text{ otherwise} \end{array} \right\}$$

$x_1, x_2, \dots, x_8$  are the values of the eight neighbors of  $p$ , starting with the east neighbor and numbered in counter-clockwise order.

**Condition G2:**

$$2 \leq \min\{n_1(p), n_2(p)\} \leq 3$$

where

$$n_1(p) = \sum_{k=1}^4 x_{2k-1} \vee x_{2k}$$

$$n_2(p) = \sum_{k=1}^4 x_{2k} \vee x_{2k+1}$$

**Condition G3:**

$$(x_2 \vee x_3 \vee \bar{x}_8) \wedge x_1 = 0$$

**Condition G3':**

$$(x_6 \vee x_7 \vee \bar{x}) \wedge x_5 = 0$$

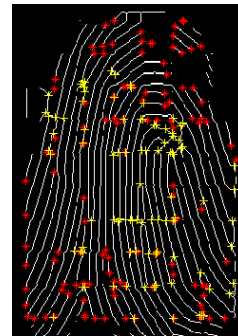


Fig. 6. Fingerprint image with minutiae points

The two subiterations together make up one iteration of the thinning algorithm. At the end of this process, the minutiae points are extracted from the fingerprint image. Then the locations i.e., coordinates of the minutiae points are acquired. The extracted minutiae points' location i.e., the coordinates are represented in a matrix A as follows:

$$A = \begin{bmatrix} X_1 & Y_1 \\ X_2 & Y_2 \\ \vdots & \vdots \\ X_n & Y_n \end{bmatrix} \tag{1}$$

Where 'n' is the number of minutiae points and X, Y represents the coordinates of the minutiae points. This coordinate matrix A is used to generate watermark in our scheme. This watermark data serves as a proof for the

ownership when ownership dispute arises. The embedding of watermark into the original image is presented in the following subsection.

### 3.2 Watermark Embedding

The original image and the minutiae's coordinate matrix A, extracted from the fingerprint image of the owner, are fed as input to the embedding process. The embedding is performed in the frequency domain. We have utilized the core concept proposed by Alexander et al. [30] for the embedding and have modified their approach to a certain extent to cater our requirements. In [30], a combination of Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) are employed for the watermark embedding and extraction process. The DCT of the original image is computed. The DCT coefficients are then mapped into four quadrants using zig-zag sequence. The

SVD of all the four quadrants is computed and the watermark is embedded only in the singular values of SVD. A brief description of SVD is given as follows:

**Singular Value Decomposition (SVD):** The application of SVD on any matrix results in three matrices namely U,  $\Sigma$  and V. The U and V are unitary matrices also known as Singular Vectors and  $\Sigma$  is the diagonal matrix which contains singular values in its diagonal. The singular value decomposition (SVD) of a matrix X is written as follows:

$$X = U * \Sigma * V^T$$

Figure 7 depicts the block diagram of watermark embedding process. In the figure  $U_X, V_X$  represent the singular vectors of original image.

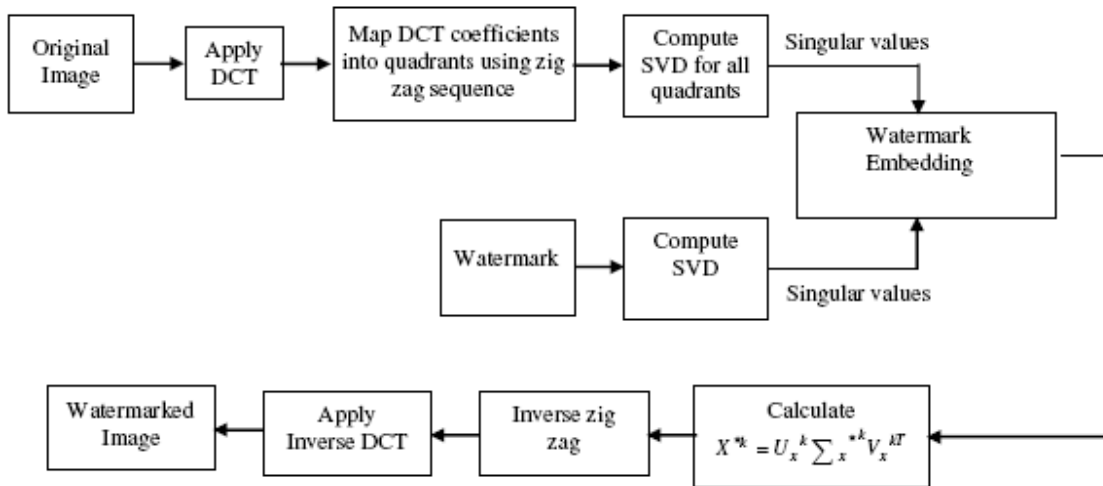


Fig. 7. Block diagram of Watermark Embedding process

The steps involved in watermark embedding are as follows:

**Input:** Original Image ( $I_o$ ), Watermark data (A)  
**Output:** Watermarked Image ( $I_w$ )

1. DCT is applied to the whole original image.
2. Four quadrants are formed from DCT transformed coefficients using zig-zag sequence.
3. SVD for all the four quadrants is computed.  $U_X$  and  $V_X$  are the singular vectors and  $\Sigma_X$  is the Singular value.

$$X^k = U_X^k \Sigma_X^k V_X^{kT}, k = 1,2,3,4$$

4. SVD for the watermark A is computed.  $U_w$  and  $V_w$  are the singular vectors and  $\Sigma_w$  is the Singular value.

$$W = U_w \Sigma_w V_w^T$$

5. Subsequently the singular values of both the original image ( $\Sigma_X$ ) and the watermark ( $\Sigma_w$ ) are considered. The following mathematical operation is performed to embed the watermark.

$$\Sigma_X^{*k} = \left( \Sigma_X^k + \Sigma_w \right) \times 0.25, k = 1,2,3,4 \quad (2)$$

The singular values of the watermark data are embedded into the singular values of the quadrants until all the watermark data are embedded. For instance, if one quadrant is not sufficient to embed the watermark, then other quadrants are used for embedding.

6. Then the modified DCT coefficients are obtained with the aid of modified singular values and singular vectors.

$$X^{*k} = U_X^k \sum_X^{*k} V_X^{kT}$$

7. The modified DCT coefficients are mapped back to their original positions
8. Inverse DCT is applied to get the watermarked image.

### 3.3 Watermark Extraction

The extraction of watermark from the watermarked image is detailed in this subsection. As the watermarking scheme proposed by Alexander et al. [30] is non-blind, the

extraction of watermark requires both the original image and the watermarked image. The DCT is applied to both the original image and the watermarked image. Then the DCT coefficients are mapped into four quadrants using zig-zag sequence. The SVD of all the quadrants are computed and the singular values of the watermark data are extracted. These singular values serve as a proof for solving the ownership dispute. Figure 8 portrays the block diagram of the watermark extraction process.

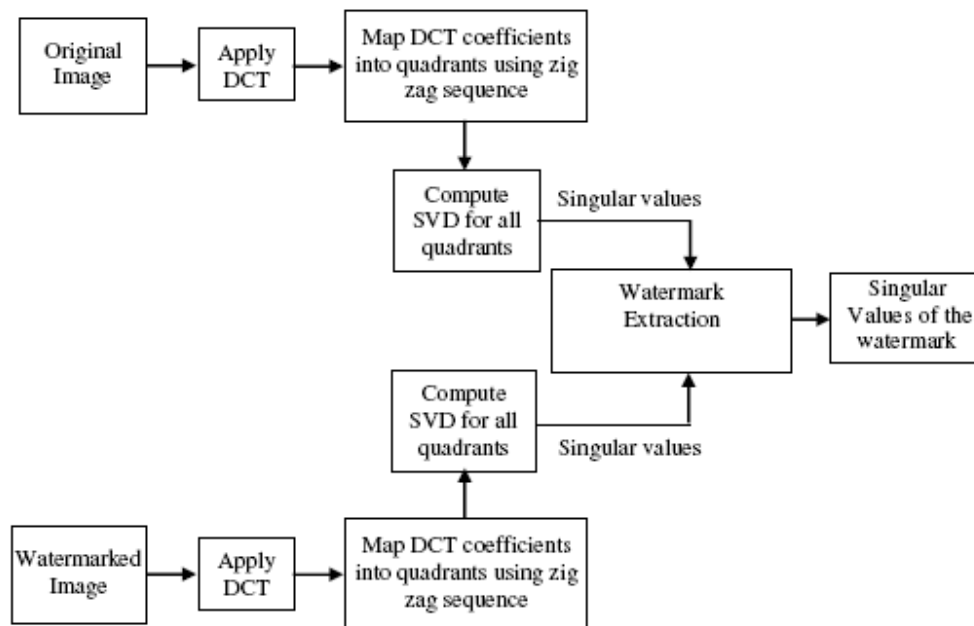


Fig.8. Block diagram of Watermark Extraction Process

The steps involved in the watermark extraction are as follows:

**Input:** Watermarked Image ( $I_w$ ), Original Image ( $I_o$ ), Watermark data Size

**Output:** Singular Values of Watermark data

1. DCT is applied to the whole original image
2. Four quadrants are formed from DCT transformed image using Zig-zag sequence.
3. Singular Value Decomposition (SVD) of all the four quadrants is computed.  $U_X$  and  $V_X$  are the singular vectors and  $\sum_X$  is the Singular value.

$$X^k = U_X^k \sum_X^k V_X^{kT}, k = 1,2,3,4.$$

4. DCT is applied to the whole watermarked image.
5. The DCT coefficients are mapped into four quadrants using zig-zag sequence.

6. SVD is applied to all the four quadrants.  $U_X$  and  $V_X$  are the singular vectors and  $\sum_X^*$  is the Singular value.

$$X^{*k} = U_X^k \sum_X^{*k} V_X^{kT} \text{ Where } k=1, 2, 3, 4$$

7. The singular values of both the watermarked image and the original image are considered and the following mathematical operation is performed.

$$\sum_A = (\sum_X^{*k} - \sum_X^k) / 0.25, k = 1,2,3,4 \quad (3)$$

The above operation is performed until all the singular values of the watermark data are extracted. The resultant singular values ( $\sum_A$ ) are the singular values of the watermark. These singular values serve as a proof for ownership verification when any sort of ownership dispute arises.



### 3.4. Ownership Verification

The verification of ownership from the watermarked image is presented in this subsection. Ownership verification is the process of assessing the rightful owner of the digital data. If any ownership dispute arises, initially the embedded watermark data, which identifies the owner, is extracted from the watermarked image. The watermark data that we have embedded is the singular values of the coordinate of the minutiae points that are extracted from the actual owner’s fingerprint image. Subsequently, the minutiae points are extracted from the claiming person’s fingerprint and its SVD is computed. If both the singular values are equal, then the person who claims is the actual owner of the image.

Let the singular values extracted from the watermarked image be  $\sum_A$  and the singular values of the coordinate of minutiae points extracted from the claiming person’s fingerprint image be  $\sum_{Ac}$ . If both of these values are similar, then we conclude that the person who is claiming is the rightful owner of the original image.

extracted from the fingerprint of the owner. The coordinates of the minutiae points were determined and represented in the form of a matrix as follows.

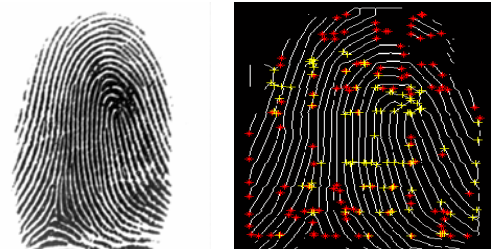


Fig 9. Fingerprint and its minutiae points



$$A = \begin{bmatrix} 171 & 17 \\ 204 & 17 \\ 234 & 17 \\ 144 & 39 \\ 145 & 46 \\ 83 & 48 \\ \vdots & \vdots \\ \vdots & \vdots \end{bmatrix}$$

## 4. Experimental Results

In this section, we have presented the experimental results of our proposed scheme. We have implemented our proposed scheme in MATLAB. The minutiae points were

The SVD of the above matrix is computed and singular values alone are embedded into the original image. The original image, watermarked image and PSNR values of the watermarked image are given in Table 1.

Table 1: Original Image, Watermarked Image and its PSNR values

Original Image	Watermarked Image	PSNR (dB)
		43.0216



		44.5467
		42.9876
		45.8234

In order to verify the ownership, the embedded watermark is extracted from the watermarked image. The embedded watermark is the singular values of the coordinates of minutiae points extracted from owner's fingerprint. Subsequently, the minutiae points are extracted from the claiming person's fingerprint and its coordinates are determined and represented as a matrix using (1). Later, the SVD of the matrix thus formed is calculated and the singular values are compared against the extracted singular values from the watermarked image. If both are similar, then the person claiming ownership is the actual owner of the image.

## 5. Conclusion

The drastic advancements in the area of digital technology have created the necessity to offer security for copyright protection of digital contents. A DRM system needs to be capable of providing relentless content protection against illegal access to the digital content, restricting access to only those with appropriate authorization. Watermarking techniques are being employed for this purpose these days. However the embedded watermark data can be easily hacked by the hackers and thus result as a threat to protection of digital content. To solve the security issues in protecting the rights of digital content, in this paper, we have presented a novel scheme, which uses watermarking and biometrics, to enhance the security of copyright protection. In the proposed scheme, the minutiae points

were extracted from the fingerprint of the owner and the coordinates of the minutiae points were determined and represented as a matrix. The SVD of the matrix was computed and the singular values were embedded into the original image. The watermark embedding and extraction were performed in DCT-SVD domain. The embedded singular values of minutiae's coordinates serve as a proof for the rightful ownership verification of the image when ownership dispute arises. Biometrics and Watermarking are themselves powerful technologies for providing security when used individually. The proposed scheme combining these two techniques and thus is highly efficient and secure.

## References

- [1] John Chirillo, Scott Blaul, "Implementing Biometric Security," John Wiley Publishers, 1<sup>st</sup> Edition, ISBN: 0764525026, 2003.
- [2] Nandakumar, K.Jain, A.K.Pankanti, S., "Fingerprint-based Fuzzy Vault: Implementation and Performance", IEEE Transactions on Information Forensics and Security, Vol: 2, No: 4, pp: 744-757, 2007.
- [3] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp., "Advances in digital video content protection.", IEEE: Special Issue on Advances in Video Coding and Delivery, pp:171-183, 2005.
- [4] Memon, N. and Wong, P.W., "Protecting digital media content," Communications of the ACM, Vol: 41, pp.35-43, 1998.
- [5] X. Xu, S. Dexter, A. M. Eskicioglu, "A Hybrid Scheme of Encryption and Watermarking," IS&T/SPIE Symposium on Electronic Imaging 2004, Security, Steganography, and Watermarking of Multimedia Contents VI Conference, Vol. 5306, pp. 725-736. 2004.
- [6] Congress of the United States of America, "Enhanced border security and visa entry reform act", 2002.
- [7] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Secure data hiding in wavelet compressed fingerprint images," In Proceedings of the ACM Multimedia Workshops , pp. 127-130, USA, 2000.
- [8] A. K. Jain and U. Uludag, "Hiding biometric data," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494-1498, 2003.
- [9] K. Zebbiche, L. Ghouti, F. Khelifi, and A. Bouridane, "Protecting fingerprint data using watermarking," In Proceedings of the 1st NASA/ESA Conference on Adaptive Hardware and Systems , pp. 451-456, 2006.
- [10] Saraju, P. Mohanty. "Digital Watermarking: A Tutorial Review". Dept of Computer Science and Engineering, University of South Florida. 1999.
- [11] Huayin Si, Chang-Tsun Li, "Copyright Protection in Virtual Communities through Digital Watermarking", Idea Group Publishing, 2005.
- [12] Daniel Socek, Michal Sramka, Oge Marques , Dubravko Culibrk, "An Improvement to a Biometric-Based Multimedia Content Protection Scheme", In Proceedings of the 8th workshop on Multimedia and security , pp.135-139, 2006.
- [13] G. Voyatzis and I. Pitas, "The use of watermarks in the protection of digital multimedia products," IEEE Proceedings, vol. 87, No. 7, pp 1197-1207, July 1999.
- [14] A.B. Kahng, J. Lach, W.H. M-Smith, S. Mantik, I.L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Constraint-based watermarking techniques for design IP protection," IEEE Trans. Comput.-Aided Des. Integrated Circuits Syst., vol.20, no.10, pp.1236-1252, Oct. 2001.
- [15] Scott Craver, Stefan Katzenbeisser, "Copyright protection protocols based on asymmetric watermarking: The ticket concept", In Communications and Multimedia Security Issues of the New Century, pp 159-170, 2001.
- [16] K. Zebbiche, F. Khelifi, "Region-Based Watermarking of Biometric Images: Case Study in Fingerprint Images", International Journal of Digital Multimedia Broadcasting, 2008.
- [17] S. Jain, "Digital watermarking techniques: a case study in fingerprints & faces", Proc. ICVGIP 2000, pp. 139-144, 2000.
- [18] G. Voyatzis, I. Pitas, "The use of watermarks in the protection of digital multimedia products," IEEE Proceedings, vol. 87, No. 7, pp 1197-1207, July 1999.
- [19] Holliman, M., Memon, N., "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes", Image Processing, IEEE Transactions.
- [20] Justin Picard, Claus Vielhauer and Niels Thorwirth, "Towards Fraud-Proof ID documents using multiple data hiding technologies and biometrics", SPIE Proceedings, vol.5306, pp: 416-427, 2004.
- [21] Minerva M. Yeung and Sharath Pankanti, "Verification Watermarks on Fingerprint Recognition and Retrieval", SPIE Proceedings, vol. 3657, no. 66, 1999, Doi:10.1117/12.344704.
- [22] Mohamed Mostafa Abd Allah, "Artificial Neural Networks Based Fingerprint Authentication with Clusters Algorithm", in proc.of Informatica vol.29, pp: 303-307, 2005.
- [23] Sooyeon Jung, Dongeun Lee, Seongwon Lee, and Joonki Paik, "Robust Watermarking for Compressed Video Using Fingerprints and Its Applications", in proc. of International Journal of Control, Automation and Systems, vol. 6, no. 6, pp. 794-799, December 2008.
- [24] Umut Uludag and Anil K. Jain, "Multimedia Content Protection via Biometrics -Based Encryption", in Proceedings of the International Conference on Multimedia and Expo, vol.3, pp: 237 - 240, 2003, ISBN:0-7803-7965-9.
- [25] Mina Deng, Lothar Fritsch, and Klaus Kursawe, "Personal Rights Management - Taming camera-phones for individual privacy enforcement", in proc. of 6th workshop on Privacy Enhancing Technologies, vol.4258, pp: 172-189, December 2006, Doi: 10.1007/11957454.x
- [26] Tuan Hoang, Dat Tran, and Dharmendra Sharma, "Remote Multimodal Biometric Authentication Using Bit Priority-Based Fragile Watermarking", in Proceedings of the 19th International Conference on Pattern Recognition (ICPR), 2008.
- [27] Emanuele Maiorana, Patrizio Campisi, and Alessandro Neri, "Template Protection for On-line Signature-based Recognition Systems", in proc. of BIOD, pp: 170-180, 2008.
- [28] Fred von Lohmann, "Fair use and Digital Rights Management: Preliminary Thoughts on the (Irreconcilable?) Tension between them", in proc. of Electronic Frontier

Foundation, March 2005, <http://www.eff.org/wp/fair-use-and-digital-rights-management-preliminary-thoughts-irreconcilable-tension-between-them>.

- [29] Ian Kerr, "Hacking@privacy: Why We Need Protection from the Technologies That Protect Copyright", in proc. of Conference on privacy and identity, 2007.
- [30] Alexander Sverdlov, Scott Dexter, Ahmet M. Eskicioglu, "Robust DCT -SVD domain image watermarking for copyright protection: embedding data in all frequencies", in Proceedings of the 13th Annual European Signal Processing Conference (EUSIPCO2005), September 2005.
- [31] Jain, A.K.; Prabhakar, S.; Hong, L.; Pankanti, S., "Filterbank-based fingerprint matching", IEEE Transactions on Image Processing, vol. 9, no. 5, pp: 846-859, May 2000, Doi: 10.1109/83.841531.
- [32] E. Hastings, "A Survey of Thinning Methodologies", Pattern analysis and Machine Intelligence, IEEE Transactions, vol. 4, Issue 9, pp. 869- 885, 1992.
- [33]L. Lam, S. W. Lee, and C. Y. Suen, "Thinning Methodologies-A Comprehensive Survey", IEEE Transactions on Pattern analysis and machine intelligence, vol. 14, no. 9, 1992.
- [34] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu, " Fingerprint Verification System using Minutiae Extraction Technique", in proc. of World Academy of Science, Engineering and Technology, vol. 36, December 2008.
- [35] Greenberg, S., Aladjem, M., Kogan, D., Dimitrov, I., "Fingerprint image enhancement using filtering techniques", In Proc. 15th International Conf. on Pattern Recognition III, pp. 326-329, 2000.
- [36] Neil Yager and Adnan Amin, " Fingerprint verification based on minutiae features: a review", in proc. of Journal on Pattern Analysis and Applications, vol. 7, no. 1A pp: 94-113, Feb 2004.
- [37] C.Johnson, P. Montague and C. Steketee, "Digital Rights Management for Content Distribution", In proceedings of Australasian Information Security Workshop 2003 (AISW2003), Vol. 21, 2003.



**Professor N.Nagamalleswara Rao** received the ME (Computer science) from M.N.R.E.C Allahabad, U.P, India, B.Tech (Electronics and communications) From Bapatla Engineering college, Bapatla AP, India. He has 18 years of teaching experience & presently working as a Prof & HOD Department of computer science at Chebrolu engineering college, Chebrolu, AP. He is a life

member in ISTE, Member of IEEE. Presently pursuing his PhD degree and his areas of interest are Security, Image processing, Biometrics.



**Prof. P. Thrimurthy** received his PhD degree from Gujarat University He has 30 years of teaching experience and presently working as Head, Department of computer science and Engineering in Nagarjuna university, Guntur, Andhra Pradesh .Served Armed Forces Head Quarters (Indian Army) Delhi & Gujarat University and Sardar Patel University

Professor of Computer Science ( Since July 1985) and served as Head, Computer Science, Chairman of Board of Studies in Computer Science, Director, University Computer Centre at both Sardar Patel University and Acharya Nagarjuna University Major / Minor Research Projects Conducted e-Governance Project: Rajiv Guntur Portal, first District Portal. Areas of Research Interest Software Engineering, & Software Security, Knowledge Management No of PhDs Guided 10, No. of Books Published 4, International journals 20, National Journals 30



**Dr. B. Raveendra Babu** received his Ph.D degree from S.V.University, Tirupati, M.S degree in Software Systems from Birla Institute of Technology and Science, Pilani, M.E degree in Computer Science & Engineering from Anna University, Chennai. He has 25 years of teaching experience and presently working as

Head, Dept of Computer Science and Engineering at RVR & JC College of Engineering, Guntur, Andhra Pradesh. He is a life member in CSI, ISTE & ACM and also member IEEE (Computer Society). He has published more than 20 research publications in various National, International conferences, proceedings and Journals.