iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 6 **Issue:** III **Month of publication:** March 2018

**DOI:** http://doi.org/10.22214/ijraset.2018.3110

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue III, March 2018- Available at www.ijraset.com*

# An Efficient Methodology for Digital Ownership Intended For Digital Media with Biometric Features

Janani.G[1], Narasimhan.C[2]
[1]*PG – Student[1], Department of ECE, Bharathidasan Engineering College, Nattrampalli, Vellore District, Tamilnadu, India*
[2] *Senior Assistant Professor[2], Department of ECE, Bharathidasan Engineering College, Nattrampalli, Vellore District, Tamilnadu, India*

***Abstract*: Every digital media that are encoded in machine-readable formats termed as Digital Media. To protect personal data stored in computers and the same which is used for digital communication needs protection and identity. In this way Digital Identity plays a major role in communication. In Multimedia, digital watermarking can be employed to get digital ownership for the digital media. In consideration with these issues, we propose to a framework which incorporates digital watermark with biometric data as the kernel. This is a watermark based technique which uses encrypted biometric data which proves ownership of digital media. With our proposed solution, each individuality will have unique watermark mechanism and this will enhance the ownership of digital media. Encrypted fingerprint images with its biometric features are generated and used as watermarking scheme. We evaluate by applying Arnold transformation to encrypt the biometric data and to embed the watermark in the image discrete cosine transformation was used. We have used MATLAB 7.14 to simulate and represent the results. The results have proven that digital media for digital media was efficient and robust.***

***Keywords*: Digital Ownership, Biometric, Digital Media, Watermarking, Secure Communication, image discrete cosine transformation.***

## I. INTRODUCTION

A watermark is a mechanism in which a mark is inserted as an entity in a paper document or in a stream of a video or image and this secretly embedded mark represents the holder of an individual. The various watermarking entities are represented in the below Fig. 1.

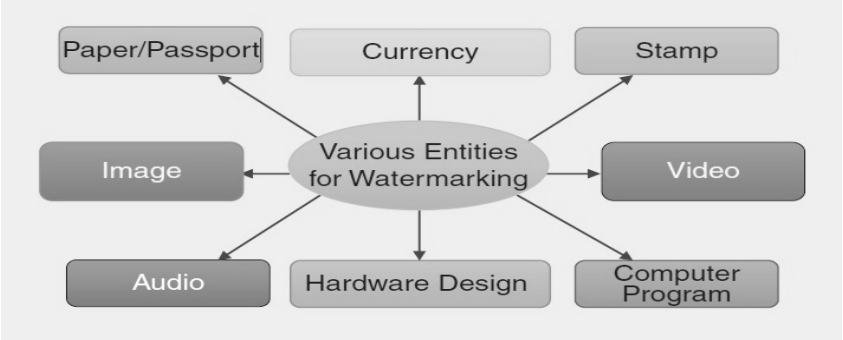



Fig. 1 The various watermarking entities

The process of embedding an unseen mark of an owner in an entity resolves the ownership conflicts process, this is termed as watermarking. The intention of watermarking scheme is to protect and secure a authentic ownership against illegal claims and distribution of copyrighted works, piracy, forgery, or theft.

Digital image refers to processing of a two dimensional picture by a digital computer. In general, digital image can be represented as an array of real or complex numbers with a finite number of bits. An image will be digitized and stored in computer memory as a matrix of binary digits. To claim ownership in digital media, a digital watermark can be used. In this paper, we propose a solution to overcome the ownership issues on any digital media. We incorporate biometric data and its features to provide secure ownership. Watermarks produced from biometric features are used to encrypt fingerprint images. In this way unique recognition can be achieved and ownership for digital content can be established. In this framework, we have shown the importance of digital

ownership for digital content in communication. The next section provides the survey followed by proposed framework with results and discussions.

## II. RELATED WORK

Watermarking is a simplified and low cost model which is used for longer time in protecting and hiding a message for secure communication in a digital form. The application which employs digital watermarking uses some algorithm to verify the ownership of an entity. The mechanism of altering the entity in a mode so that only the correspondent dispatcher and anticipated receiver will be allowed to use and understand the message embedded in it. Getting a digital ownership for digital media is mostly unsecure in the existing approaches. We have compared and represented the schemes used for various watermarking mechanisms in the survey.

In paper [2], they proposed to compact with the content protection problem in the DIBR 3D images which uses a novel blind multiple watermarking schemes. Their results have shown that their proposed methodology is better and robust when comparing with JPEG compression and various noise adding attacks.

In paper [3], a watermarking method with the DIBR generated from new viewpoint video frame was proposed and employed. They have represented the results and shown that their proposed solution solves the issues related to watermarking which uses the new viewpoint video frame which does not affects the quality of the image generated by DIBR.

A spread-spectrum-like discrete cosine transform domain (DCT domain) [7] watermarking method for copyright safety of immobile digital images is analysed in this paper. The DCT was deployed on 8*8 pixels blocks in the JPEG algorithm. They have performed two tests namely: watermark decoding and watermark detection. A generalized Gaussian distribution was applied to statistically reproduce the DCT coefficients of the unique image. The process performed in paper [7] is shown below in Fig. 2 and Fig. 3.

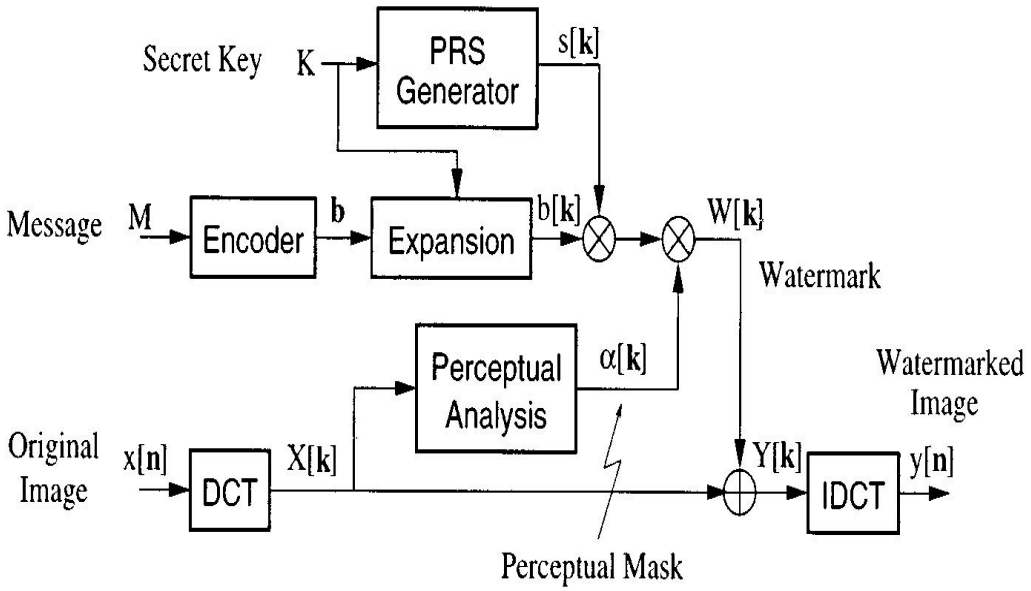



Fig. 2 Watermark Embedding Process

In the digital watermarking community, a watermark conflict to geometric attacks is a most important issue to be resolved. Most of the measures in the literature focuses on the common problems of affine transforms like scaling, translation and rotation. The robust features are less/more related to the corresponding pixel position is the major problem in the existing watermarking techniques. An image based watermarking mechanism [4] was proposed by considering two statistical features – the histogram shape and the mean in the Gaussian filtered low-frequency component of images.

An efficient and robust method was presented in paper [5]. This is a new informed image watermarking scheme which provides high level of sturdiness and reduces the complexity level at a rate of 1/64 bit/pixel. This proposed methodology uses Taylor series and Hidden Markov model (HMM) in the wavelet domain. Then a new HMM-based spherical code is constructed to offer an efficient tradeoff between robustness and deformation.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue III, March 2018- Available at www.ijraset.com*

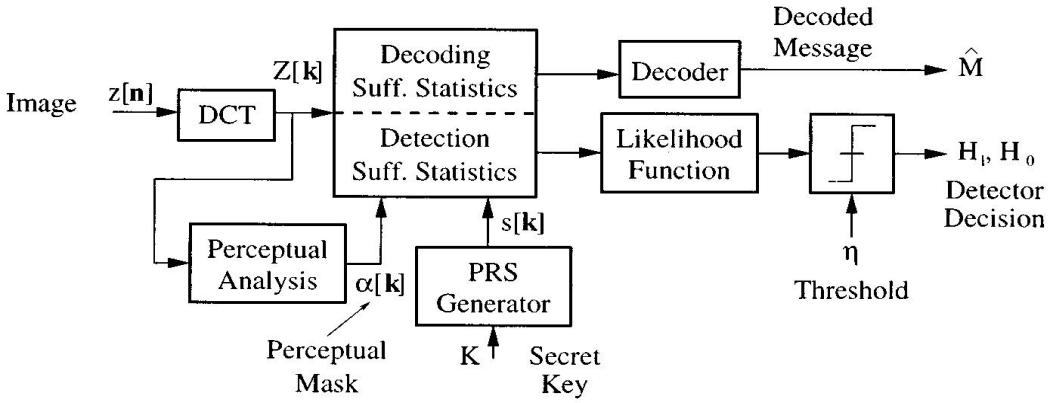



Fig. 3 Watermark Verification Process

Few of most used watermarking algorithms are Patchwork-based watermark, Watermarking by histogram specification. All the existing watermarking schemes use a Pseudo random number sequence or chaos based watermark or an image. These watermarking mechanisms may not be owned for ownership. There were limitations in getting the authentic ownership for the digital media and the existing methods do not address an efficient methodology to address this issue.

We propose to make use biometric features of encrypted fingerprint images to generate watermarks. By doing this, sole credentials can be achieved and this provides a secure ownership of digital media since biometric features are distinctive for each and every humans. We use Arnold transformation and DCT for secure ownership. To encrypt the biometric data Arnold transformation was used and to embed the watermark in the image discrete cosine transformation was used. We have discussed the implementations and results in the next section.

## III.PROPOSED METHODOLOGY

In our proposed scheme, the features of the biometric data were incorporated as the kernel of the digital watermark. The prerequisites of a digital watermark will be met using the biometric data. This watermarking will be unique for every individual and this helps in proving the secure ownership of their digital content, this was one of the advantages of the proposed scheme. A watermark with biometric features will be having a clear brand of ownership. An Image Processing System was represented in Fig. 4. The proposed scheme was simulated using MATLAB 7.14, which is a high-performance language for technical computing. This provides an easy-to-use and flexible background to solve the problems and express the solutions in a familiar manner. This also can be used to deploy mathematical notations. MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This helps us to answer many complex technical problems, particularly related to matrix and vector.

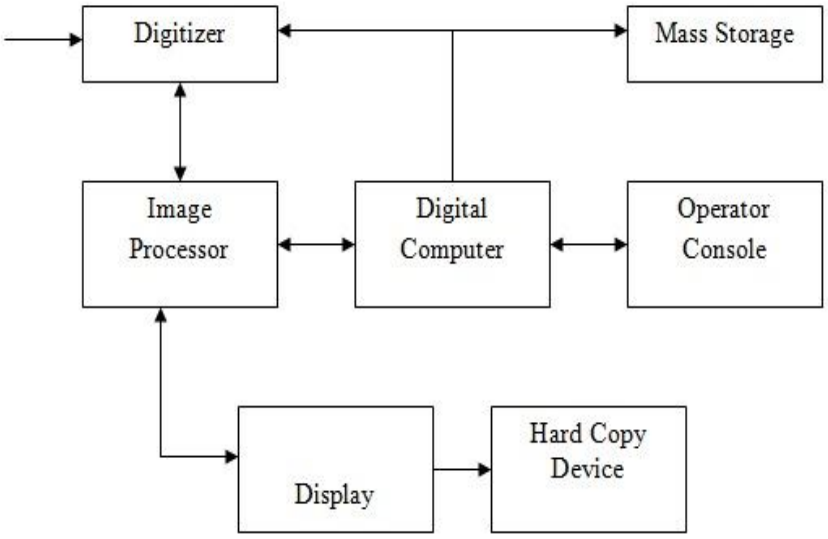



Fig. 4 Image Processing System

The watermarking protection scheme is illustrated in the Fig. 5.

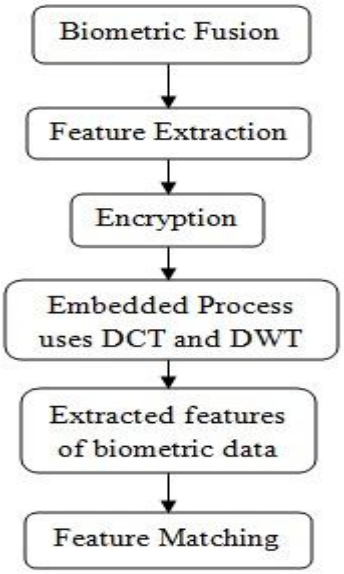



Fig. 5 Process Involved in Watermarking Protection Scheme

*A. Multi Model Biometric Fusion*

1) *Finger Print:* The fingerprint area in the image was first cropped to enhance the quality of the image and histogram equalization was performed to increase the perception information. This was performed to get better dissimilarity in the image by diversifying their intensity values over the entire cropped image.
2) *Retinal:* This stage is the crucial stage where we perform the pre-processing to the raw input images here convert the input colour images into corresponding gray images and invert the gray image into inverted green channel in order to make the blood vessel to be more visible.
3) *Fingervein:* Rotational and translational variations are felt as noisy in the acquired fingerprint images. So images are pre-processed under three stages. 1) ROI Segmentation, 2) Translation and position arrangement and 3) Enhancement of image to extract the patterns. As a result, to segment the ROI from the original image binary mask was used. Finally, the biometric enhanced data was combined.

*B. Chaotic Encryption*

Arnold Cat Map was employed to perform shearing and wrapping process to absolutely scramble a matrix subsequent to much iteration. This was a one to one mapping mechanism.

*C. Feature Extraction*

To mine the features from the iris image, a Haar wavelet technique was used. The features of the image are extracted and the localization of the inner iris boundary is performed using Hough transformation. Discrete Haar Wavelet Transform (DHWT) was used for extracting the features of the image.

*D. Watermarking*

A watermarking scheme based on biometric data was developed using an algorithm based on discrete cosine transforms (DCT). This divides an image into dissimilar frequency bands and makes much simpler to use middle frequency bands of an image for embedding process in watermarking.

*E. Feature Matching*

Euclidean distance or Euclidean metric is the normal straight line distance between two points. L2 norm or L2 distance is the global term for the Euclidean norm.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue III, March 2018- Available at www.ijraset.com*

$$d(\mathbf{p},\mathbf{q}) = d(\mathbf{q},\mathbf{p}) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \cdots + (q_n - p_n)^2}$$

$$= \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2}.$$

## IV. RESULTS AND DISCUSSIONS

The proposed framework was implemented in MATLAB and the results are represented in the following figures. Fig. 6 represents the input image and the encrypted image. The image will be get encrypted with a secret data information which will be secure in communication.

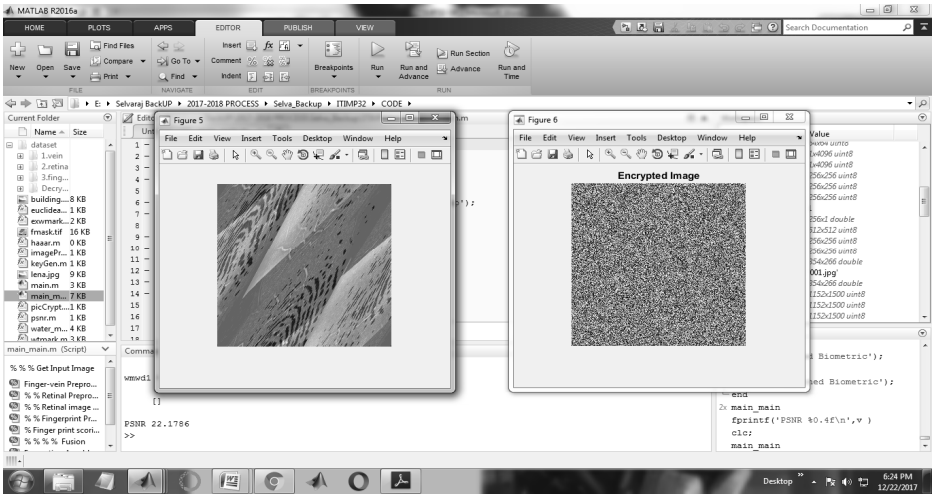



Fig. 6 Encrypted Image

The watermarked and the image which was decrypted on the receiver side were shown in Fig. 7. The biometric features used which will be unique to individual and with this features secure way of information exchange can be achieved. The embedded information cannot be accessed by the receiver without any authentic biometric features. Digital ownership for any digital media can be claimed in a safe and secure manner. Decryption process makes the receiver to retrieve the secret embedded information in a secure manner. Feature Extraction and identification was given in Fig. 8.

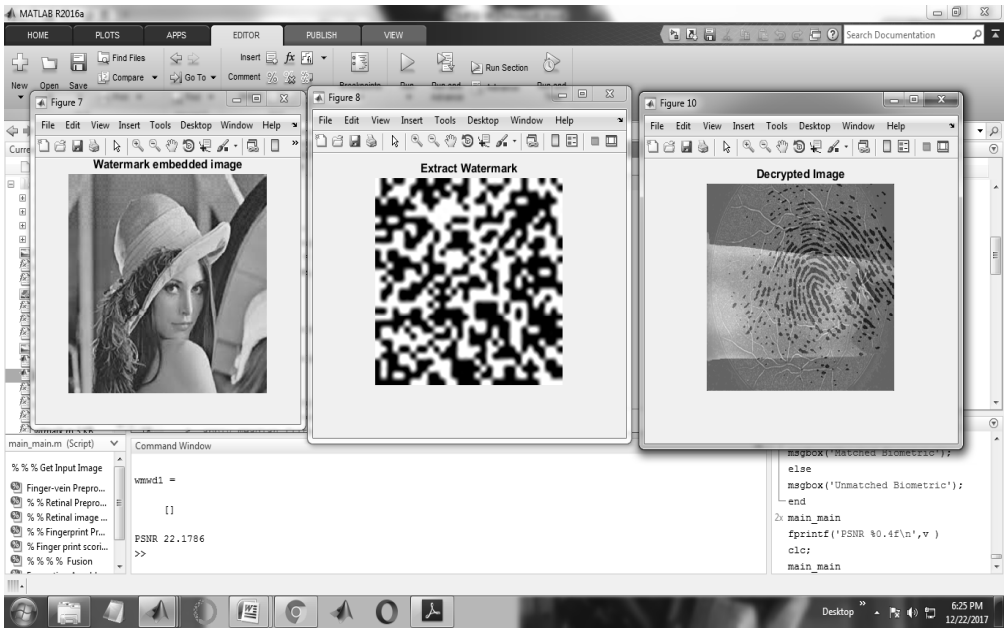



Fig. 7 Watermarking and Decryption

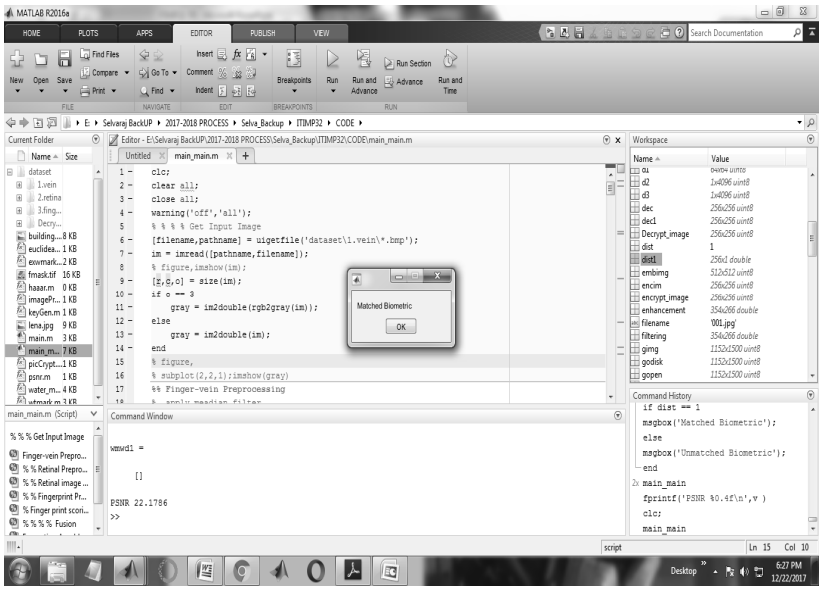


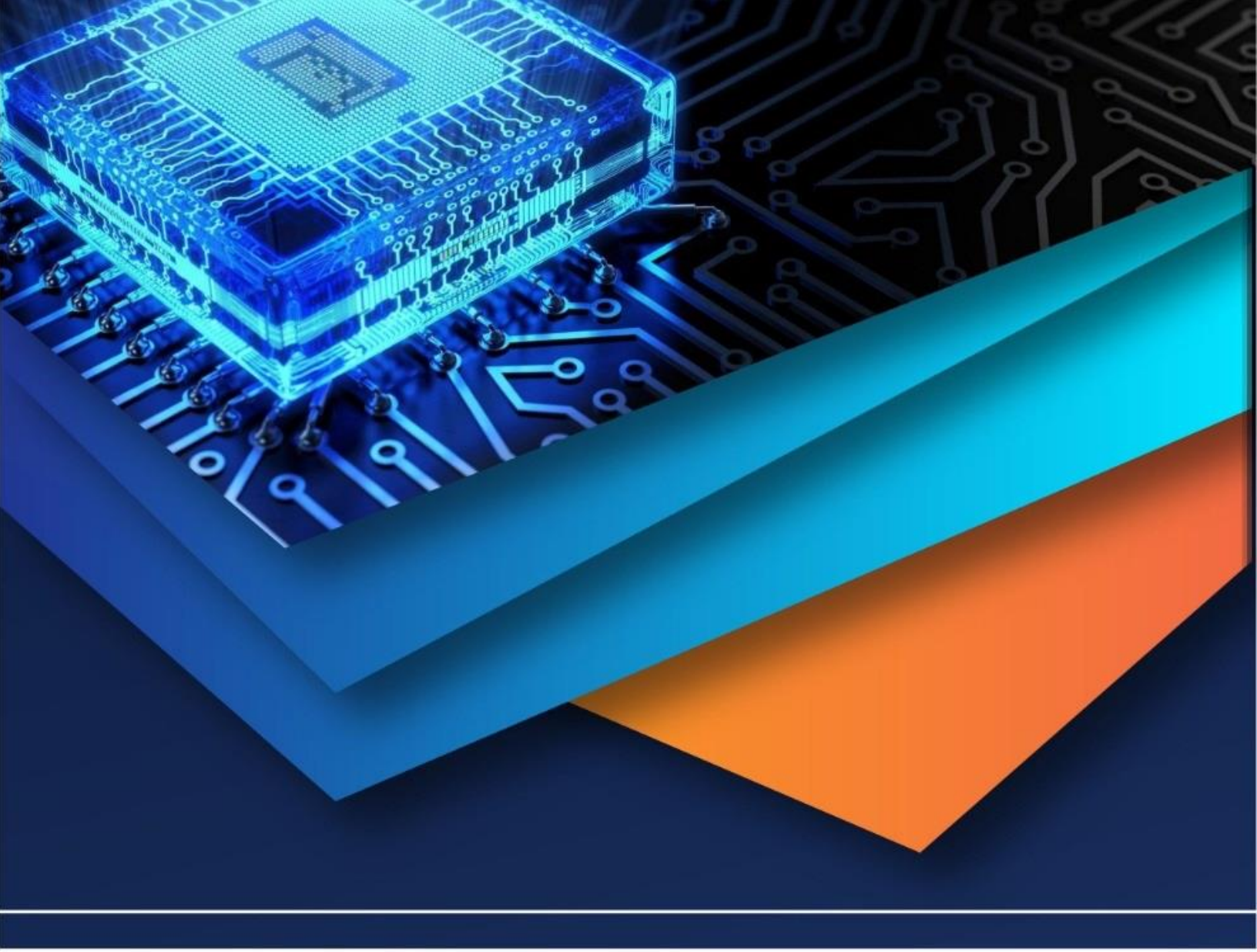

Fig. 8 Feature Identification

## V. CONCLUSION

A secure watermarking technique was deployed with the features of biometric encrypted fingerprint image. The same was used as digital watermarking in this proposed scheme. This ensures the ownership of the digital media which used biometric information; this is not open to the elements of any risk and security, which were enhanced to provide better results. The validation of this technique was through by means of a DCT based watermarking method. The extracted feature points are mapped individually for identification. Digital ownership for the digital content can be achieved with our methodology and also this scheme was authentic and secure. In future, we plan to discover more efficient methods to encrypt and to enhance the biometric features for making digital ownership for digital media.

## REFERENCES

[1] Malay Kishore Dutta, Anushikha Singh, K.M.Soni, Radim Burget, Kamil Riha, "Watermarking of Digital Media with Encrypted Biometric Features for Digital Ownership", IEEE, 2013.
[2] AsYu-Hsun Lin and Ja-Ling Wu, "A Digital Blind Watermarking for Depth-Image-Based Rendering 3D Images,"IEEE Transactions on Broadcasting, VOL. 57, no. 2, 2011, pp-602-611.
[3] N. Zhu, G. Ding, and J. Wang, "A novel digital watermarking method for new viewpoint video based on depth map" in 8th Int. Conf. Intell. Syst. Design Appl. (ISDA), Nov. 2008, vol. 2, pp. 3–7.
[4] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain" IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 6, pp. 777–790, Jun. 2008.
[5] Chuntao Wang, Jiangqun Ni, and Jiwu Huang, "An Informed Watermarking Scheme Using Hidden Markov Model in the Wavelet Domain" IEEE Transactions on Information Forensics and Security, VOL. 7, NO. 3, 2012, pp.853-867.
[6] G. Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol. 17, pp 20-43, September 2000.
[7] J.R. Hernandez, M.Amado, and F. Perez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performanc Analysis And a New Structure", in IEEE Transaction on Image Processing, vol. 9, pp 55-68, 2000.
[8] Malay Kishore Dutta, Phalguni Gupta and Vinay K. Pathak "Blind Watermarking in Audio Signals using Biometric Features in Wavelet Domain", International Conference of IEEE Region 10, TENCON 2009, 2009, pp-1-5.
[9] Malay Kishore Dutta, Phalguni Gupta and Vinay K. Pathak "Biometric Based Unique Key Generation for Audio Watermarking"- International Conference on Pattern Recognition and Machine Intelligence, LNCS, Vol. 5909, 2009, pp- 458-463.
[10] Malay Kishore Dutta, Phalguni Gupta and Vinay K. Pathak "Audio Watermarking Using Pseudorandom Sequences Based on Biometric Templates"- Journal of Computers, Vol. 5, No. 3, 2010, pp. 372-379.
[11] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, "Handbook of Fingerprint Recognition" - Springer, New York, 2003.
[12] Jianghong Bao, Qigui Yang "Period of the discrete Arnold cat map and general cat map" Nonlinear Dyn (2012) 70:1365–1375.
[13] Dyson, F., Falk, H. "Period of a discrete cat mapping" Am. Math. Mon. 99(7), 603–614 (1992).
[14] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security," EURASIP Journal on Advances in Signal Processing, vol. 2008, p. 17, 2008.
[15] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, no. 3-4, 1996, pp. 313–336.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY