International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)

Impact Factor: 5.858 (SJIF-2019), e-ISSN: 2455-2585

Volume 6 , Issue 3 , March -2020

Colour Image Watermarking based on Wavelet and QR Decomposition

Divya Audichya [1] Dr.Vikas Soni [2]

[1]M.Tech, Department of Digital Electronics,
[2] Professors, Department of Electronics & Communication Engineering,
Rajasthan Technical University, Modi Institute of Technology, Kota, Rajasthan

Abstract: Water marking is becoming an indispensible tool for modern copy right protection & secure communications of hidden data. Embedding water marking in Image / video or digital data is norm of the day, to prove ownership & copy right protection. However there are a number of security threats to water marking, such as unauthorized extraction, removal, tampering of cover media etc. The system proposed is a highly secure video water marking system which is secured by using combination of Biometrics, Stegnography & cryptography. The watermark is encrypted using mixed key cryptography. The private key used for encryption is generated by fingerprint of authorized person. Another unique feature of the proposed system is that private key may not be pre-shared or sent on a transmission channel, as it can be regenerated at the receiver side using biometric authentication.

Keywords: Video Watermarking, Biometric Random key Generation, Mixed Key Cryptography, LSB Watermarking

I. INTRODUCTION

A digital watermark is a kind of marker, which is embedded in a noise-tolerant signal such as audio, video or image data. It is usually used to identify ownership of the copyright of such a signal. "Watermark" is the act of hiding digital information in a carrier signal; the hidden information should, but need not, be related to the carrier signal. Digital watermarks can be used to verify the authenticity or integrity of the carrier signal or to indicate the identity of its owner. It is mainly used to track copyright violations and to authenticate banknotes. Like conventional physical watermarks, digital watermarks are often only perceptible under certain conditions, i.e. H. After using an algorithm. If a digital watermark distorts the carrier signal so that it is easily perceptible, it can be considered less effective depending on the purpose. Conventional watermarks can be applied to visible media (such as images or videos), while digital watermarks can be audio, images, video, text or 3D models. A signal can carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal. The required properties of a digital watermark depend on the application in which it is used. To mark media files with copyright information, a digital watermark must be fairly robust to changes that can be applied to the carrier signal. If integrity needs to be ensured, a fragile watermark is applied instead. Both the steganography and the digital watermark use steganographic techniques to covertly embed data in noisy signals. While steganography aims to ignore the human senses, the digital watermark tries to control robustness as a top priority. Since a digital copy of the data is identical to the original, the digital watermark is a passive protection tool. It only marks data, but does not deteriorate it and does not control access to the data. One application of the digital watermark is source tracking. A watermark is embedded in a digital signal at each distribution point. If a copy of the work is later found, the watermark can be retrieved from the copy and the source of the distribution is known. This technique has been reported to be used to determine the source of illegally copied films.

II. OBJECTIVES OF STUDY

[1.] Design & Development of a Hybrid Algorithm for Watermarking of Color Images Using Wavelet Decomposition, QR Code Decomposition, Cryptography, & other allied techniques.

[2.] Design of Suitable Algorithms for Improving the Recovery Probability of Watermarks in Tampered, Cropped & Noisy Images.

[3.] Design of Suitable Algorithms for Handling Compression of Watermarked Images Using Various Lossy & Lossless Methods.

[4.] Development of Multi-Faceted Algorithm for Watermarking of Various Media such as Grayscale Images, Color Images & Audio Streams in Color Images.

[5.] Usage of Multi-Bit Vector Stegenography Techniques For Watermarking Multiple Media In a Single Cover Image.

[6.] Usage of Advanced Cryptography Regimes For Enhancing Security of the Embedded Watermarks & Avoid Unintended Recovery.

[7.] Extension of the Above System To Allow For Color Video To Be Watermarked With Multiple Media With Enhanced Cryptographic Security.

III. EXISTING TECHNIQUES

This study presents a watermarking scheme that uses RDWT in combination with SVD to protect copyrights. Our scheme uses modified entropy to determine the embedding areas with less distortion. Arnold Transform encrypts a watermark image to provide additional security for confidential information. The encrypted watermark is embedded in the host image by examining U3, 1 and U4, coefficients obtained from RDWT-SVD used on the host image. Our scheme is tested against various types of signal processing and geometric attacks. The test results of our scheme show an improvement in SSIM and NC values compared to other existing schemes. The proposed scheme confirms satisfactory results, however, due to the Arnold transformation and the RDWT, our scheme requires little higher computing costs. This can be accepted as our goal is to improve the robustness against different types of attacks. [1]

Data exchange over the Internet and the widespread use of digital media has increased remarkably. The growing interest in digital watermarks in the past decade is certainly due to the increasing need for copyright protection. The applications of video watermarks in the areas of copy control, radio surveillance, fingerprint, video authentication, copyright protection, etc. are increasing immensely. The main aspects of hiding information are capacity, security and robustness. The ability of anyone who discovers the information is security, and robustness refers to the resistance to changes in the coverage content before hidden information is destroyed. Video watermarking algorithms usually prefer robustness. With a robust algorithm, it is not possible to remove the watermark without a severe deterioration in the coverage content. In this article, we introduce the concept of video watermarking and the functions required to design a robust video with watermark for a valuable application, and focus on different areas of video watermarking techniques.

Technology the watermark design and the insertion of watermarks do not include any transformations. Simple techniques such as adding or replacing are used to combine watermarks with the host signal and embedding is done directly in the pixel domain. The watermark is applied in the pixel or coordinate domain. The main strengths of pixel domain methods are that they are conceptually simple and have very little complexity. As a result, they have proven to be the most attractive for video watermarking applications where real-time performance is a primary concern. However, they also have some significant limitations: The need for absolute spatial synchronization leads to a high susceptibility to de-synchronization attacks. The lack of consideration of the temporal axis leads to a susceptibility to video processing, and the optimization of multiple image collusions and watermarks is difficult only with spatial analysis techniques. In the article, we revised various video watermarking techniques proposed in the literature in different areas. It is expected that new approaches will come out and merge existing approaches. For example, cascading two powerful mathematical transformations; the discrete wavelet transform (DWT) and the singular value decomposition (SVD). The two transformations are different transformation domain techniques and therefore offer different but complementary degrees of robustness against the same attack. [2]

This paper proposes an algorithmic video watermarking scheme in the area of discrete wavelet transform (DWT). The scene change analysis is performed first to split the video into different scenes. DWT transforms every frame of the video into a wavelet domain. The watermark image is broken down into 8-bit levels, encrypted and embedded in the medium-frequency DWT coefficients. The quality of the video with watermark is improved by GA. Experimental results show that it is robust against frequent video watermark attacks such as frame drop, frame averaging, additive noise, and lossy compression. In this article, I propose a scene-based watermarking scheme. The scheme is robust against various attacks since neither original videos nor videos with watermarks are required to restore original videos and watermark videos. Experiments with these novel video watermarking schemes were conducted to test the performance of a show. The robustness of our approach is demonstrated by the calculation of the NC. [3]

Digital video content is now readily available on the Internet and various media. Thanks to easy availability, digital videos have become more popular than analog media. And it gets a keen eye on its property. Property integrity can easily be violated with various video editing programs. In this context, we propose a chip-level framework in accordance with our previously proposed LSB framework for videos, with which a colored watermark logo can be embedded in the video images of a video content. The quality of the original video is not affected, since the color watermark is perceptibly invisible to the human visual system (HVS) in videos with watermarks. Since we propose a blind extraction scheme, no prior knowledge of this watermark or the original video is required at the time of extraction. Security is also used with a hash function and a secret key. If a counterfeiter tries to watermark extraction with an inappropriate key, he receives a video frame that resembles the noise. We have informally referred to our proposed chip as the BLIND CHIP because we used the blind extraction method. The robustness of the proposed framework is also proven against various deliberate attacks.

A detailed experiment was carried out and it was found that our proposed framework can embed color watermarks in video sequences in a very efficient way and also ensure the quality of watermarked videos is consistent. In videos with watermarks, the watermark is perceptibly invisible to HVS. The extraction was carried out blind, i. H. Neither the watermark nor the original video is required at the time of watermark extraction. The security problem has been expanded to include a secret key and a hash function. The chip-based solution also improves portability, which leads us to a wider horizon like mobile communication. Our proposed system has proven to be robust against deliberate attacks. The limitation of the proposed system is the high computational complexity and the need for uncompressed video for embedding watermarks. For this reason, the proposed framework is not suitable for real-time video streaming such as broadcast monitoring, in which the watermark is embedded and extracted in real time. However, our system is ideal for other areas of application such as copyright protection, fingerprinting, copy control of DVDs and television programs that are not encoded and broadcast in real time. As a future research scope, we will expand our proposed framework on video compression such as MPEG-4, MJPEG, etc. [4]

The sudden surge in interest in watermarks is most likely due to increasing concerns about content copyright protection. With the rapid growth of the Internet and multimedia systems in distributed environments, digital data owners can now more easily transmit multimedia documents over the Internet. However, current technology does not properly protect its copyrights. This has generated widespread interest in multimedia security and multimedia copyright protection and has become a major concern of the public in recent years. In the early days, encryption and control access techniques were used to protect media ownership. Recently, watermarking techniques have been used to keep copyrights safe. In this work, a fast and secure invisible video watermarking technique was presented. The technique is mainly based on DCT and low frequency using a pseudorandom number (PN) sequence generator for the embedding algorithm. The system was implemented with VHDL and the results verified with MATLAB. The implemented watermark system is implemented with the Xilinx chip (XCV800). The implementation results show that the total area of the watermarking technique is 45% of the total FPGA area, with the maximum delay being 16.393 ns. The experimental results show that the two techniques have a mean square error (MSE) of 0.0133 and a peak signal to noise ratio (PSNR) of 66.8984 dB. The results were demonstrated and compared to traditional watermarking techniques using DCT. Watermarking is a copy protection system that can be used to trace illegally produced copies of the protected multimedia content. The main advantage of watermarks is that the watermark is permanently embedded in visual data of the content, but at the expense of a small loss of fidelity. After recognizing the importance of multimedia security and video watermarking in today's internet world and reviewing the latest audio watermark, image watermark, and video watermarking technologies, a video watermarking scheme is proposed. [5]

Robust, invisible double digital watermarking technology is currently becoming the most popular and challenging direction. It has caused great concern in the international community in recent years. The individual watermark algorithms always have only one function. To overcome the disadvantages, a multipurpose algorithm with two watermarks is presented, which is based on wavelet transformation and image partition. The algorithm embeds both robust watermark and fragile watermark in a video sequence using DWT and several embedded methods. The fragile watermark later embedded is used for the early robust watermark. The test results show that the proposed algorithm is more robust and imperceptible and can at the same time achieve copyright protection and content authentication.

This article introduces a video dual watermark algorithm that offers the advantages of strong robustness for a robust watermark and sensitive manipulation and manipulation localization for fragile watermarks. It encrypts binary images using chaotic encryption technology.

HVS selectively embeds the watermark in blocks, which is more mysterious to the human visual system, increases the watermark's shear capacity, and improves the invisibility of the watermark. Experimental results show that the algorithm resolves the contradiction between robustness and invisibility and has good robustness against shear, JPEG compression and noise attacks. [6]

In this paper, an adaptive video watermarking scheme for H.264 was proposed. First, introduce the idea of secret sharing into the scheme of the watermark generation algorithm. then we propose a secret image release method derived from the (t, n) threshold scheme. The original watermark is broken down into n copies of the shadow. Choose a shadow as the watermark to embed. The remaining n-1 copies of the shadow are saved for the verification key. The proposed method can save many redundancies. Based on the (n, n) threshold scheme, we propose a blind video watermark scheme in the DCT area. The value of the selected coefficient is adaptively modified in accordance with the energy value of neighboring coefficients and the binary watermark bits. The experimental results show that this method improves the robustness of the watermark while maintaining the high video quality. [7]

Digital video is one of the most popular multimedia data that is exchanged on the Internet. Due to its perfectly reproducible nature, many illegal copies of the original video can be made. Methods are needed to protect the owner's copyrights and prevent illegal copying. A video can also be exposed to multiple deliberate attacks, e.g. B. frame drop, averaging, cropping, and median filtering, as well as accidental attacks such as adding noise and compression, which can compromise copyright information and deny authentication. This article suggests the design and implementation of scene-based watermarks where extraction is a blind method. The developed method embeds 8 bit plane images, which were obtained from a single gray scale watermark image, in different scenes of a video sequence. With this algorithm, some of the light values in the video images are selected and divided into groups, and the watermark bits are embedded by adjusting the relative relationship of the member in each group. A sufficient number of watermark bits are embedded in the video images without noticeable distortion. The watermark is also correctly retrieved in the extraction phase after various types of video manipulation and other signal processing attacks. As multimedia becomes more popular and more accessible, copyright and ownership issues also play an important role. The design and implementation of a blind watermark algorithm for uncompressed video is proposed. The algorithm successfully embeds watermark bits in the bit plane in the luminous pixel value for each video frame. The scene change detection algorithm is used to detect scenes in the video. The same bit level image is embedded in each scene and another scene contains a different bit level image. The extraction process is blind and the watermark can be extracted from the watermarked frame without distortion. Experimental results show that the proposed technique is robust against attacks such as frame drop, temporal shifts and addition of noise. [8]

Due to the extensive use of digital media applications, multimedia security and copyright protection have become enormously important. Digital watermark is a technology used to protect the copyright of digital applications.

This article introduces a compressive approach to digital video watermarking. When a watermark image is embedded in the video frame, each video frame is broken down into fields using the 2-stage discrete wavelet transform (DWT) and principal component analysis (PCA) is applied for each block in the two bands LL & HH. [1,2] Combining the two transformations improved the performance of the watermark algorithm. The scheme is tested by various attacks. The experimental result shows no visible difference between the watermark image and the original video image. It shows robustness against a wide range of attack such as Gaussian noise, salt and pepper noise, median filtering, rotation, cropping, etc. The proposed scheme is tested using the number of video sequences tested. Its experimental result shows a high imperceptibility if there is no noticeable difference between the watermark video frame and the original video frame. Without attacking noise on the watermark video frame, the calculated normalized correlation (NC) 1 and the peak signal to noise ratio (PSNR) is a high value of 44.097. The algorithm implemented using DWT-PCA is robust and inherently imperceptible. Embedding the watermark in the LL sub band helps to increase the robustness of the embedding process without significantly affecting the video quality. [9]

In this paper, author present a novel, fast and robust video watermarking scheme for uncompressed RGB-AVI video sequences in the field of discrete wavelet transformation (DWT) using Singular Value Decomposition (SVD). Scene change detection is carried out for embedding. The singular values of a binary watermark are embedded in the singular values of the LL3 sub band coefficients of the video images. The resulting signed video shows good quality. In order to test the robustness of the proposed algorithm, six different video processing operations are carried out. The high calculated PSNR values indicate that the visual quality of the signed and attacked video is good.

The low bit error rate and the high normalized cross-correlation values indicate a high correlation between the extracted and the embedded watermark. The analysis of the time complexity shows that the proposed scheme is suitable for real-time application. The conclusion is drawn that the embedding and extraction of the proposed algorithm are well optimized. The algorithm is robust and shows an improvement over other similar reported methods. In the present work a new fast and robust DWT-SVD-based video watermark algorithm is proposed. The singular values of the LL3 subband coefficients are modified by the singular values of the binary watermark image. The low temporal complexity of the proposed algorithm makes it suitable for the watermarking of videos in real time. The calculated values of all parameters are in the expected range. The perceptible quality of the video images is very good, which is indicated by high PSNR values. Watermark recovery is also good, which is indicated by high cross-correlation values and a low bit error rate between embedded and extracted watermarks. The conclusion is drawn that the embedding and extraction of the proposed algorithm are well optimized. The algorithm is robust and shows an improvement over other similar reported methods. [10]

Data exchange over the Internet and the widespread use of digital media has increased remarkably. The growing interest in digital watermarks in the past decade is certainly due to the increasing need for copyright protection. The applications of video watermarks in the areas of copy control, radio surveillance, fingerprint, video authentication, copyright protection, etc. are increasing immensely. The main aspects of hiding information are capacity, security and robustness. The ability of anyone who discovers the information is security, and robustness refers to the resistance to changes in the coverage content before hidden information is destroyed. Video watermark With robust algorithm algorithms it is usually not possible to remove the watermark without a severe deterioration of the cover content. In this article, we first conduct a survey of available video watermarking techniques and then conduct a comparative analysis based on the robustness and computing power of various watermarking algorithms.

We have come to the conclusion that robustness, geometric attack, insensitivity, PSNR (Peak Signal to Noise Ratio) and NC (Normalized Correlation) are the most important requirements for a watermark system. Different parameters are taken into account in the performance analysis for different watermarking techniques shown in this document. From the literature research, the performance is correspondingly poor, acceptable and well analyzed. Looking at this paper, one can say that the DWT (Discrete Wavelet Transform) and PCA (Principle Component Analysis) techniques are superior in performance to other techniques. [11]

Today's Internet offers great convenience when transferring large amounts of data in different parts of the world. However, the security of remote communication remains an issue. To solve this problem, the need for copyright protection has increased. The use of video watermarks in the areas of copy control, broadcast monitoring, copyright protection, video authentication, fingerprint, annotations, etc. is increasing immensely. The main goals of the video watermark are unrecognizability, robustness and capacity of hidden data. Video watermarking algorithms usually prefer robustness. In this article, techniques used in video watermarking are discussed with the literature review, and then the shortcomings are analyzed. Finally, a suggestion for new points for hiding watermarks in the video is given. This article examines various video watermarking techniques previously available from researchers. After the investigation, however, it is concluded that the previous techniques are not as efficient to provide security and that these techniques are very common in the field and therefore can be easily recognized by hackers. Watermark extraction inserted into videos. Therefore, there is a need for a new robust technique that is able to hide watermarks in such places in frames so that they cannot be extracted easily and offer more security compared to old video watermarking techniques. As new research in the same field, an algorithm with efficient point finding is proposed to hide watermarks in videos and thus provide a robust and secure watermark. [12]

IV. METHODOLOGY

System Block Diagram

4.1 Biometric Key Generation

4.1.1 Fingerprint Minutia Extraction

First we input fingerprint image and apply binarized image method and binarized the image then make the image thinning. Find minutia and remove minutia false, Select region of interest manually and automatically orientation of image in which we detect degree and tilt of images. Then validation of image and expert minutia.

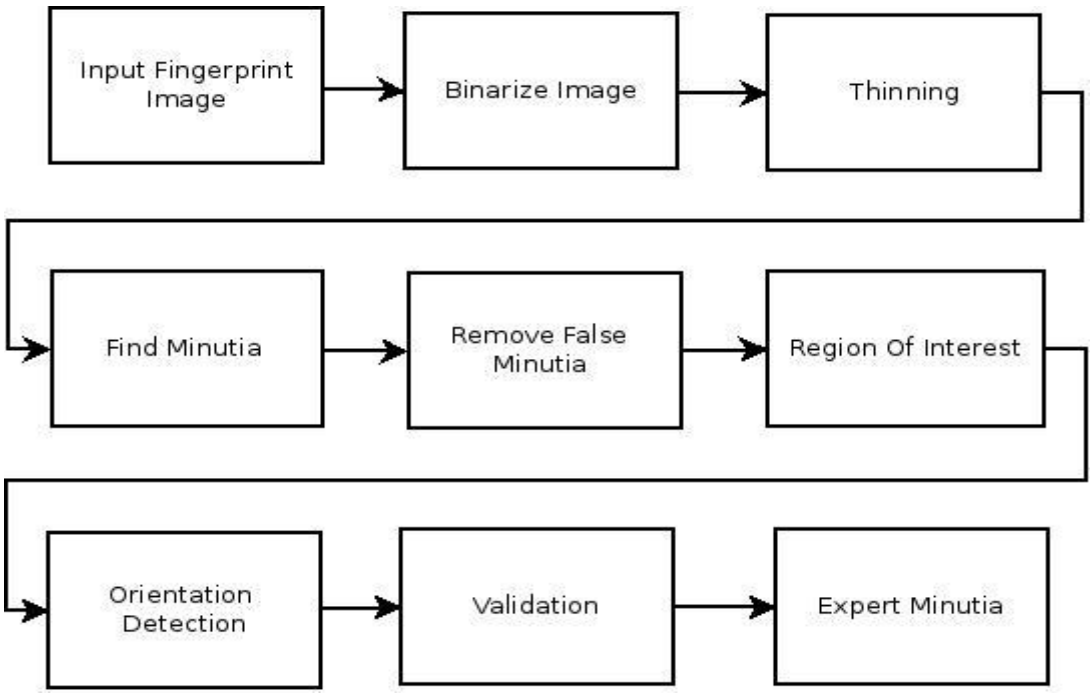

Figure 4.1 - Fingerprint Minutia Extraction

4.1.2 Minutia Based Key Generation

First we read minutia text file and read line from file then accumulate number in result. Refine random seeds; refine zero matrix of binary key size. Apply mathematical constraint for key value update and finally private key generated.

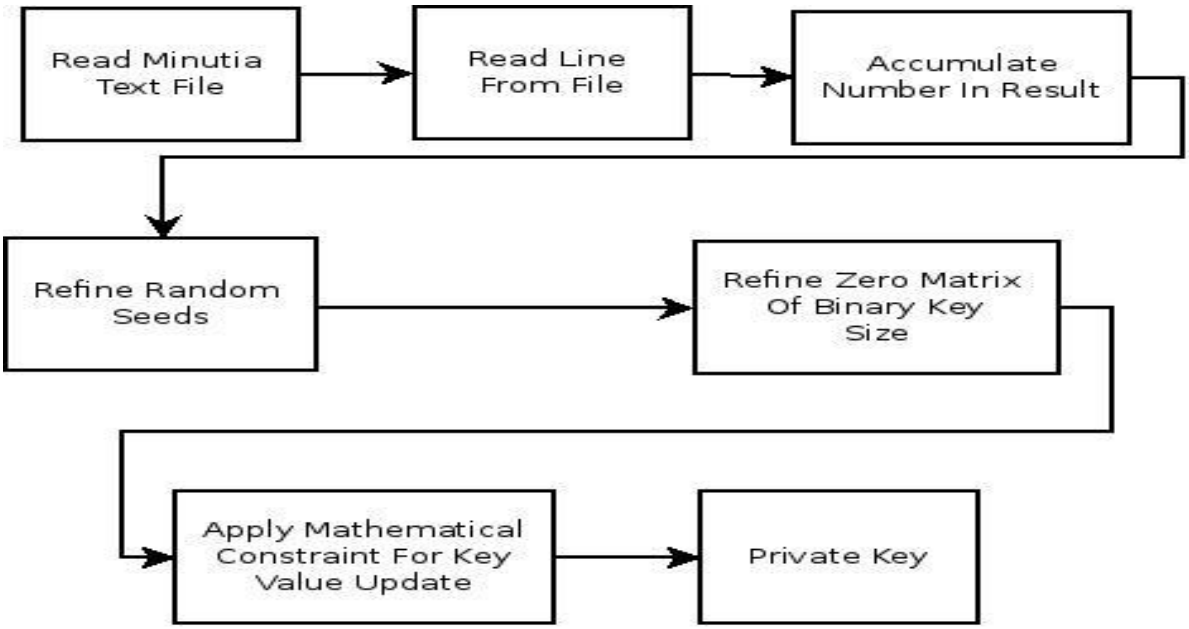

Figure 4.2 - Minutia Based Key Generation

4.2 Encode

Read video original file, bifurcate frames and select image embedding frame. Select secret image and private key then apply variable length mixed key cryptography. Replace embedding frame then reassemble video after that video encoded.

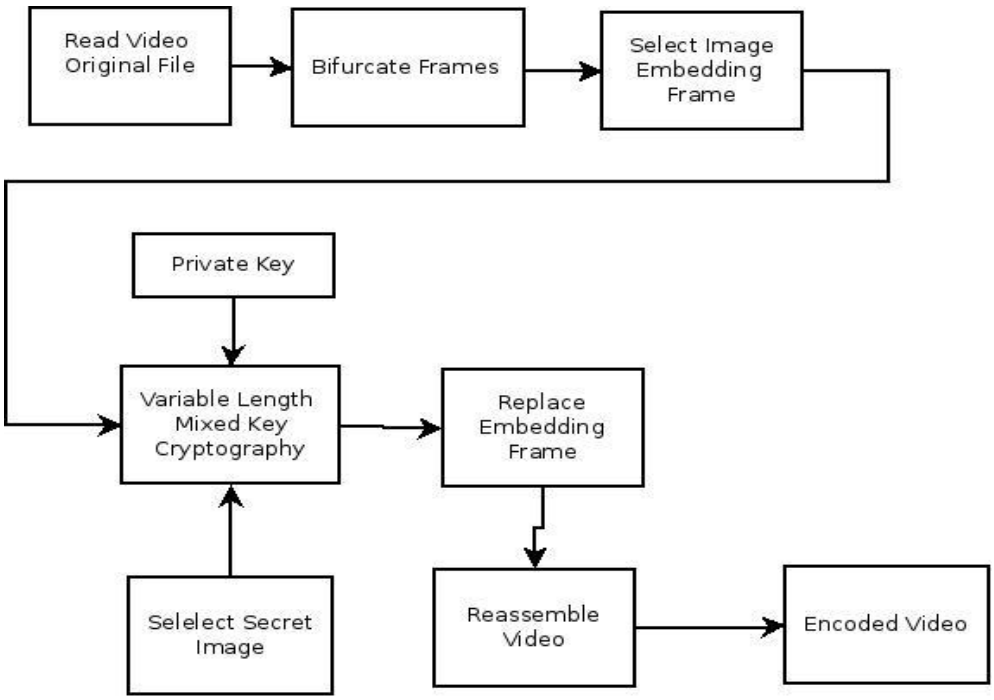

Figure 4.3 – Encode

4.3 Decode

First we read encoded video and bifurcate frame, select image decoding frame and biometrically regenerated private key and apply decryptography. Then make secret image and reassemble the video after this we recovered the video.

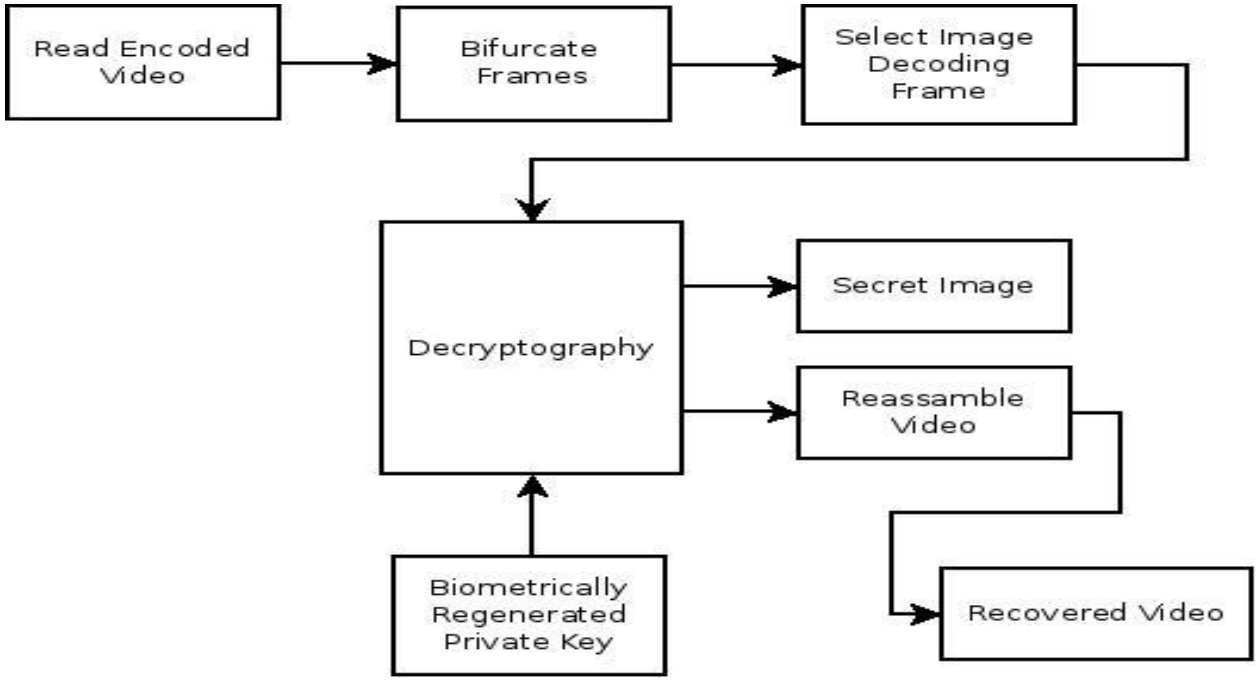

Figure 4.4 - Decode

V. RESULTS

Encode:

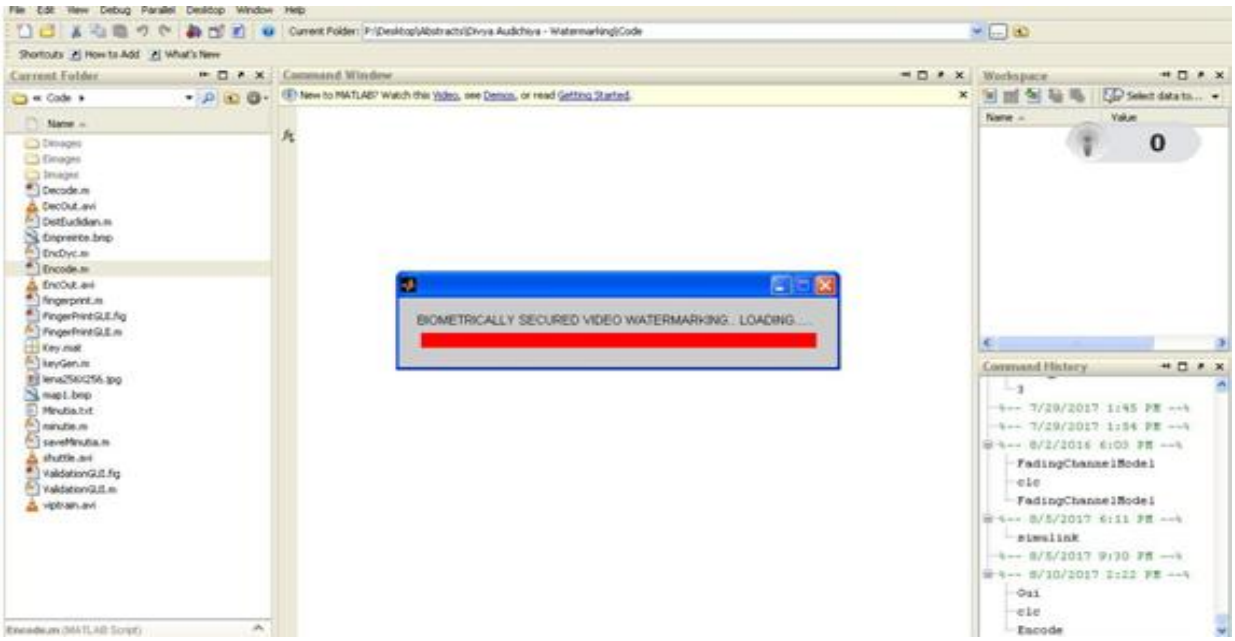

Figure 5.1 – Loading biometrically secured video watermarking

In above figure we select the file encode.m and click on right to run. Biometrically secured video watermarking

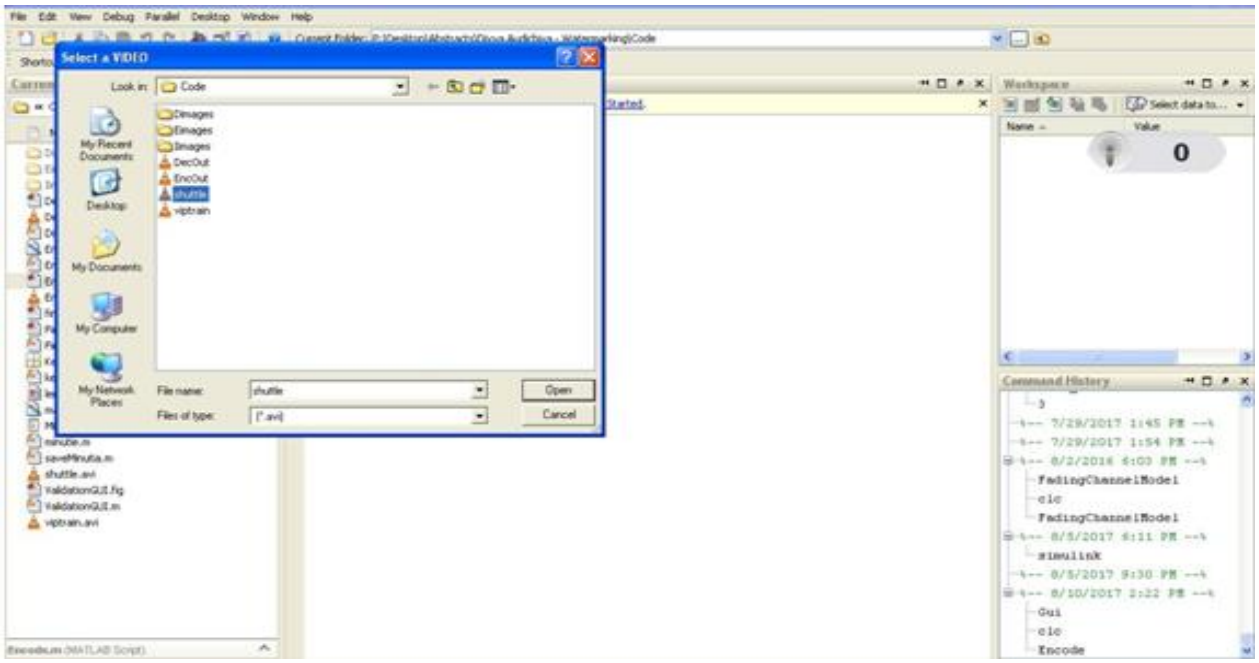

Figure 5.2 – Select the file shuttle

In above figure we open the folder of video file Select the file shuttle.

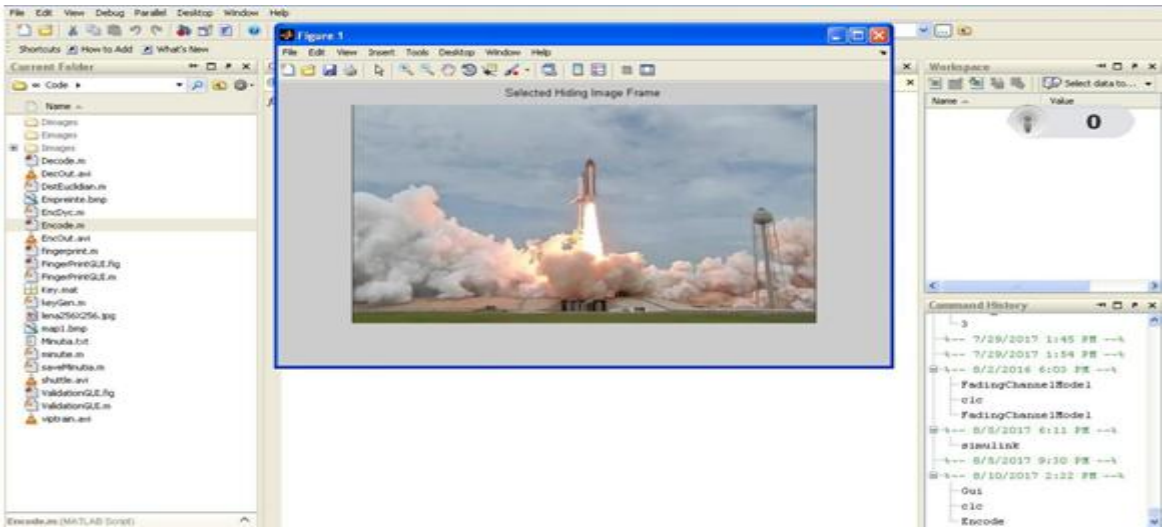

Figure 5.3 – Display the selected hidding image frame

In above figure we open the folder of image file Select the file img42. Display the selected hiding image frame.

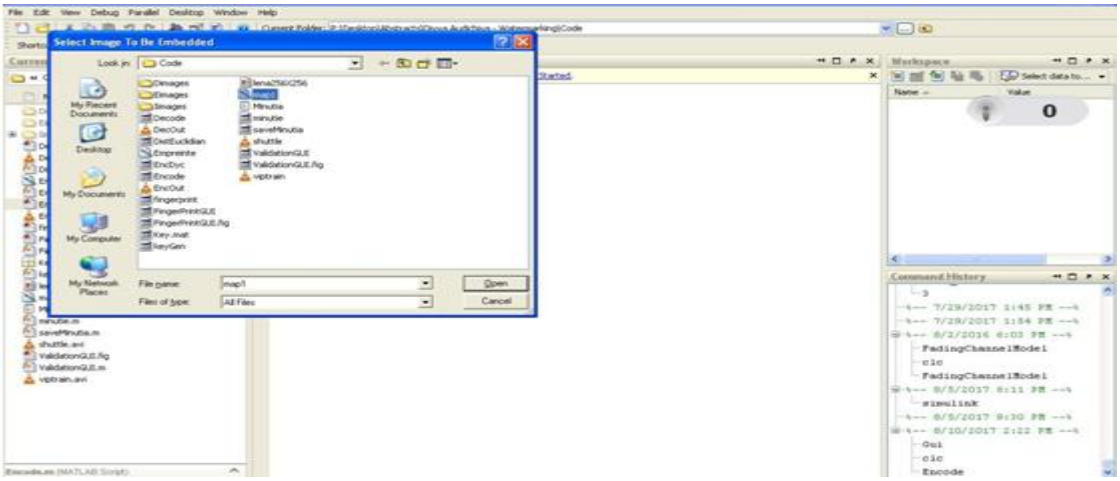

Figure 5.4 – Select the file map1

In above figure we open the folder of image and select image to be embedded and Select the file map1.

Figure 5.4 – Display selected image to be embedded on map.

In above figure we open the folder of image and select image to be embedded and Select the file map1. Display selected image to be embedded on map1.

Decode:

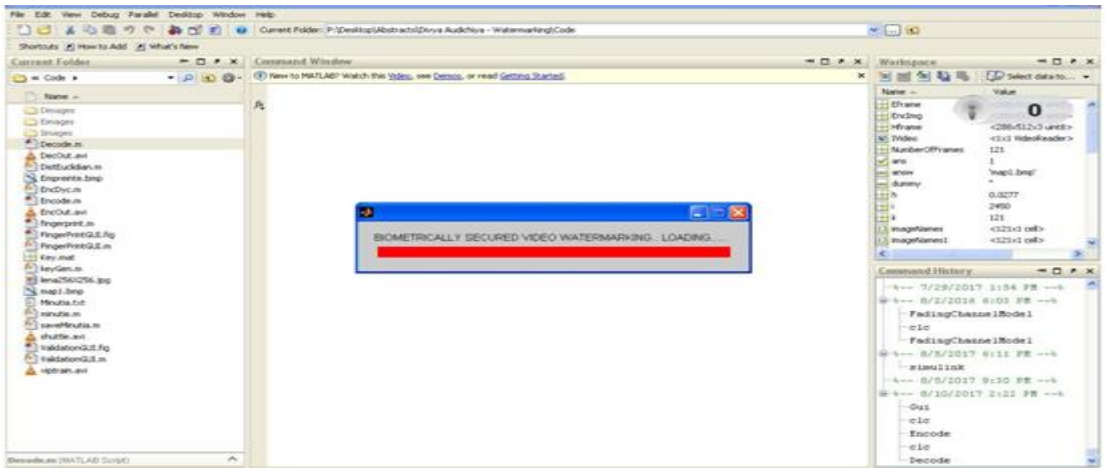

Figure 5.4 – Loading biometrically secured video watermarking

In this window we can see a loading biometrically secured video watermarking.

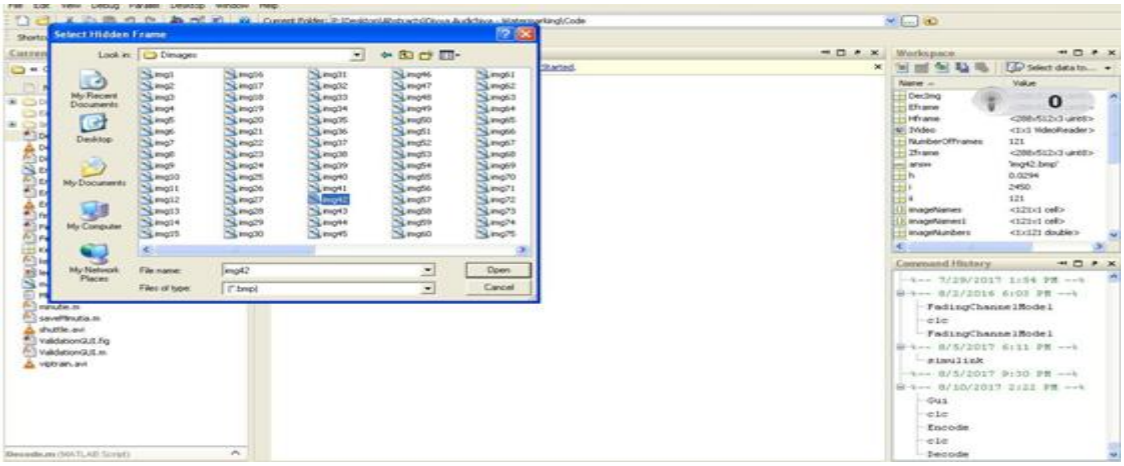

Figure 5.5 – select file img42

In this window we can see our selected image file name is img42.

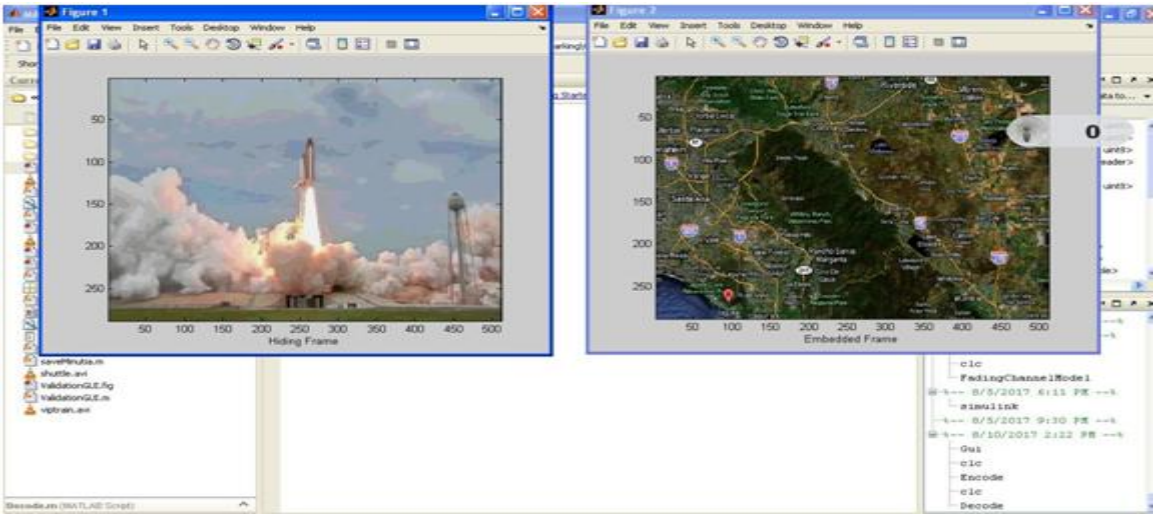

Figure 5.6 – Display hiding frame and embedded frame

In this window we see our encoded hiding frame and embedded frame image.

CONCLUSIONS

The proposed system demonstrated a highly secure video water marking system with biometrically secured private encryption key. The video to be water marked is broken into individual frames, & unique frame(s) are selected for water marking. The water mark to be embedded is encrypted by mixed key cryptography, using biometric fingerprint generated private key. The usage of biometric finger print in key generation increases key uniqueness manifolds. Also the method of key generation using biometrics enables, private key to not be shared previously, rather private key can be generated at the time of decoding using biometrics of authorized person. The proposed system provides enhanced security to video water marking as water mark is encrypted before embedding in a pre selected frame, thus for on unauthorized receiver, the embedded watermark, pretends as a random noise, which renders its detection & extraction difficult. Further level of difficulty in unauthorized extraction is implemented by using user selected random frame for water marking instead of using every and or fixed frames for the some. Further unauthorized extraction attempts are failed as the private key is generated using biometrics such as fingerprint which are unique in nature to every person, & thus increase the uniqueness quotient of the private key manifolds. The entire system has been implemented successfully as demonstrated by the results above.

FUTURE SCOPES

The proposed system has demonstrated increased levels of security, but with the enhancement in water mark detection & computerized deciphering techniques, along with massively accumulating computing power, there is a constant need to be one step ahead of security challenges. One of the proposed improvements is the usage of multiple biometric features in conjunction with fingerprint, such as retina scan or face recognition, with one used for key generation & other for authentication. Another interesting amendment can be distribution of frame numbers according hand prints or distribution of water mark in various facts of image, according to fingerprint etc.

REFERENCES

[1.] Ferda Ernawan, Muhammad Nomani Kabir, " A Blind Watermarking Technique using Redundant Wavelet Transform for Copyright Protection" ©2018 IEEE.

[2.] Rini T Paul, "Review of Robust Video Watermarking Techniques" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" 2011.

[3.] Snehal V. Patel, Prof. Arvind R. Yadav, "Invisible Digital Video Watermarking Using 4-level DWT" National Conference on Recent Trends in Engineering & Technology, 13-14 May 2011

[4.] Soumik Das1, Pradosh Bandyopadhyay, Dr. Monalisa Banerjee3, Prof. Atal Chaudhuri, "Uncompressed Video Authentication Through A Chip Based Watermarking Scheme" 2011 IEEE.

[5.] WESSAM SAYED MOHAMED SAYED EL-ARABY, "VIDEO WATERMARKING IMPLEMENTATION BASED ON FPGA" ARAB ACADEMY FOR SCIENCE, TECHNOLOGY AND MARITIME TRANSPORT (AASTMT) January 2012

[6.] Zhang Yong-mei, Ma Li, Xing Xiu-juan, "A Multi-purpose Video Watermarking Algorithm Based on Wavelet Transform and Image Partition" 2012 IEEE.

[7.] Xiaohong Li, Keke Hu, Guofu Zhang, Jianguo Jiang, Zhaopin Su, "An Adaptive Video Watermarking Based On Secret Image Sharing" © 2012 IEEE.

[8.] Venugopala P S, Dr. H. Sarojadevi, Dr. Niranjan N., Vani Bhat, "Video Watermarking by Adjusting the Pixel Values and Using Scene Change Detection" IEEE 2013

[9.] Mr Mohan A Chimanna 1, Prof.S.R.Khot, "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery" (IJERA)Vol. 3, Issue 2, March -April 2013.

[10.] Bhavna Goel, Charu Agarwal, "An Optimized Un-compressed Video WatermarkingScheme based on SVD and DWT" ©2013 IEEE

[11.] Gopal Prasad, Atul Kumar Singh, Arun Kumar Mishra, "Digital Video Watermarking Techniques and Comparative Analysis : A Review" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 11, November – 2013.

[12.] Paramjit Kaur, Dr. Vijay Laxmi, "Review on Different Video Watermarking Techniques" IJCSMC, Vol. 3, Issue. 9, September 2014.