Arnold Cat Map Based Fragile Video Watermarking Algorithm

Nihil R[1], Ajily Rachel Varghese[2], Hari S[3]
[1]Dept of ECE
[2, 3]Assistant Professor, Dept of ECE
[1, 2, 3] Mount Zion College of Engineering

Abstract- *In this paper, a delicate watermarking algorithm is introduced on a local domain to ensure the integrity of digital video content. Watermark is a video that has been duplicated to have the same size as the video frame size. Prior to embedding, the watermark is encoded in XOR encoding with a random image thus increasing security. A random image is created using a conflict map called Arnold Cat Map. By converting the pixel values of video frames, encrypted watermark is applied. The results show that the algorithm is able to detect and create locally converted video frames.*

Keywords- ACM, Embedding algorithm, Extraction algorithm Fragile Video Watermarking, Tamper Detection

I. INTRODUCTION

Digital video is a type of digital video that contains more details than an image. One photo is just a frame and digital video has picture and audio frames (if any). Digital data for example video is easily copied, transferred, edited, modified or misused. Video integrity changes whenever digital video is used. In some cases, we need to know the authenticity of the video. For example, the court needs to decide whether the video is true or not.

Fragile watermarking provides a way to verify video authenticity. With a weak watermarking approach, the watermark (data signal) is incorporated into the hosted video into a video with a watermark without affecting its cognitive quality. Watermark can also be extracted from video with watermark. When a video with a watermark is used using software, the extracted watermarked is broken. Compared to a real watermark, a broken watermark is an indication that the video has been changed.

Most research on delicate watermarking is specialized in photography. However, we can also measure a weak watermarking system for video sequencing. A video is basically a set of frames where the frame is an image, so we can embed a watermark on each frame. Based on the watermark encryption domain, digital watermarking schemes can be categorized into a local domain and transform the domain.

In the spatial domain, watermarking is done by directly changing the pixel values of the hosting video. Watermark bits are included in pixel values. Digital watermarking on the tranform domain is done by converting the transform coefficients of the host image [1] [2]. Before installing the watermark, the host image (local domain) is converted into a conversion domain using a specific modification such as DCT, DWT, DFT, etc. Conversion coefficients are enhanced by embedding watermark bits [2] [3]. Performing watermarking on a conversion domain is much more powerful than a local domain for harmless attacks.

The solution to the problems of copyright protection, copyright, illegal copying, and tracking of video transactions by Robust video watermarking in transform domain is. The watermark in the video is hard to remove with a vicious and harmless attack. On the other hand, weak video watermarking is ideal for solving video content acquisition problem. when the video is used. watermark on weak video Strength is not a problem of fragile watermarking.

II. RELATED WORKS

Elgamal [1] introduced watermarking of fragile video in terms of block mean and modulation factor. Depending on the number of watermark bits, his original video is converted from the RGB model to the YCbCr model, and the Cr-component is divided into unconventional pixel blocks,. Watermark is a binary image with characters embedded in each block separately. No key is enabled for embedding or deleting watermark. The algorithm can detect disruptive attacks such as sorting and geometric / non-geometric modifications.

Rupali [5] introduced a system of obvious vulnerabilities that are used in the public to embed and extract a watermark from the Discrete Cosine Transform domain. There are two watermarks where the first watermark is a digital signature frame and the second watermark is block numbers and frame numbers. A digital signature is used to detect interference and a second watermark helps to detect disturbed regions. Watermark embedding uses a private key, while watermark embedding uses a public key. Those who do

not know the public key can perform a watermark release. By changing the value of one pixel to the block effect where the disturbed block can be detected. While, the proposed method is not strong against congestion.

Zhi-yu [3] introduced a weak watermarking system to prove color video authenticity. First the video is converted from the RGB model to the YST model. The T element is then divided into 4 × 4 blocks. The watermark, called the authentication code, is made with an equated Discrete Cosine Transform Coefficient and embedded in the final non-zero coefficient of DCT. Watermark embedding and extracting public key usage, so those who know the public key can embed and extract watermark Results show that the system can detect interference in video with watermark.

Rinaldi Munir and Harlili unveiled a delicate watermarking algorithm on a local domain to ensure the integrity of digital video content. Watermark is a dual binary image to have the same size as the frame of the video frame To increase security watermark is encrypted with XOR-ing it with a random image. Random image created using Arnold Cat Map. Encrypted watermark embedded by converting pixel values of video frames. Some attacks have been made on video with watermark and the results show that the algorithm is able to detect and make the modified domain of video frames very well.

The security feature is not met by all monitoring schemes. One method does not use the key at all, while others use the public key to extract the watermark. Those who do not know the public key can perform a watermark release. We therefore need an optimization program so that the embedding and removal of watermark is done by the authorized group only the owner of the video.

III. PROPOSED SYSTEM

A. *Video Fragile Watermarking*

Fragile watermarking has become an exciting topic of research. Recently digital video is much easier to convert using commercial software, so there is a need to prove the authenticity of the video content. The Fragile watermarking algorithm consists of two processes: embedding and extraction. The embedding process receives input such as digital video, digital watermark, and key. To remove a watermark from a video, the user provides input such as a video with watermark, key, and real watermark. The output watermark is compared to the actual watermark and a decision is made to determine if the video is corrupted or true.

B. *Arnold Cat Map (ACM)*

Arnold Cat Map is a 2-D revolutionary map that transforms an object from one place to another in the same space [6]. In other words, ACM transforms coordinate (x, y) from an image N × N pixels to a new coordinate (x', y'). The iteration equation is

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & b \\ c & bc+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \quad \text{MOD N} \ldots\ldots\ldots (1)$$

ACM is reversible, i.e the transformed image can be returned to its original image with the equation:

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} 1 & b-1 \\ c & bc+1 \end{pmatrix} \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} \quad \text{MOD N} \ldots\ldots\ldots (2)$$

The parameters b and c are the corresponding opposing numbers, and the matrix shortcut must be 1 so that the transition effects keep the position, that is, remain in the same image position. ACM is repeated m times and each iteration produces an image that looks random. The values of b, c, and m can be considered as secret keys. After repeated times p, the image will be converted back to the original image, as shown in the Diagram. The p value varies for each image, depending on b, c, N. According to a study by [6] Freeman J. Dyson and Harold Falk found that T <3N.

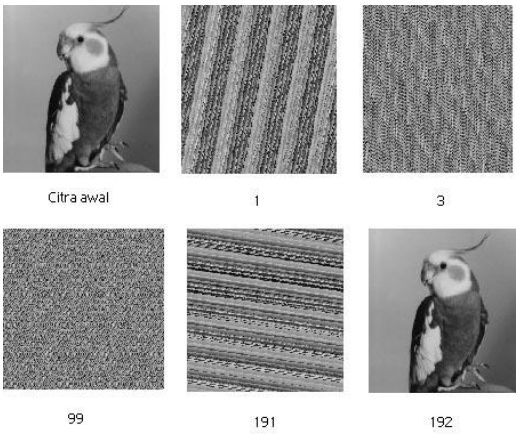

Fig 3.1. Results of iteration of ACM[7]

C. *Proposed Algorithm*

The proposed algorithm is simple and can detect deception of video frames up to a pixel level. At the local domain, embedding and extraction of watermark is performed. To find and paste corruption in video with watermark, we need a real watermark. Watermark is a digital video. However,

the watermark size may be less than the frame size of the video, so the watermark needs to be reproduced several times to produce a new watermark with the same size as the host video frame size.

To increase security, the new watermark is encoded by XOR to insert it with a random image before embedding. A random image is made by moving the binary image randomly using Arnold Cat Map (ACM). A map is created for each watermark. ACM parameters are b, c, and iteration number m. Different parameters will result in a different random image. The new watermark is encrypted with a random image using XOR functionality to produce an encrypted watermark. After that, we embed the encrypted watermark on the hosting video. Because the new watermark has the same size as the frame size, we can see changes in video frames at pixel level. From this definition, we can create a simple, yet secure, weak video algorithm. The algorithm consists of two processes: embedding algorithm and extraction algorithm, each of which will be described below.

Encryption Algorithm:-

Input: host file (v), watermark video file (w), encryption key (m)
Output: watermarked video

Step 1: Read watermark video frames w, and encryption keys. If the video has audio, then split the audio.
Step 2: Merge RGB components into a video watermark video.
Step 3: Copy a single watermark frame to produce a new watermark w ’of the same size as the managed video frames.
Step 4: Navigate w ’using arnold transform to produce a random image
Step 5: frame the video to the final draft of the watermark video to produce a new watermark video for us
Step 6: Read the hosted video file frames (v) and watermark video with us
Step 7: Embed the enclosed watermark frame on each video frame with a slight deceleration (LSB) pixels. If the frame has R, G, and B objects, then embed each item. After completing one frame and reading the next frame, consider what is going on until the final draft is completed
Step 8: If the original video is audio, combine it with watermark-framed frames to produce video with watermark.

Decryption Algorithm:-

Input: Watermark video file (v ’), Encryption key (m), Total frames (f)
Output: an extracted watermark video

Step 1: Read video frames v ’and encryption key (m)
Step 3: Assemble the LSB pieces into the watermark frame w ’’.
Step 4: Remove the encryption of the watermark w’s frame obtained by the inverse arnold transform
Step 5: remove the RGB part from w ’and generate the first frame of the watermark RGB wd.
Step 6: write wd as watermark video.
Step 7: if the frame value is less than f then go to step 1, otherwise write the last video released for the watermark.

IV. RESULT

After the watermarking algorithm was created, we applied the algorithm to a computer program. In this algorithm, the ACM parameters handle the keys. The embedding and removal of watermark can only be done by an authorized group. If the recipient does not have the keys, the issued watermark does not match the actual watermark. This algorithm therefore provides a security feature. If a video with a watermark is not controlled, modified, or interrupted, then we will find the extracted watermark is exactly the same as the actual watermark. It is an indication that the video's authenticity is verified and we conclude that the video is authentic.

To detect and validate a frame attack, one idea is to embed the frame number as the watermark information in the current frame, as the watermark details extracted from the video represent the details of the video frame number. If the extracted watermark can match the number of frames, it indicates that the video is not under attack by frame. Alternatively, frame attacks can be determined based on the relationship between a specific watermark and the frame number.

Based on our watermarking process, authentication code is used to detect intraframe interruptions, and watermark is used to detect dangerous activities, such as insertion and removal between frames. To test the algorithm's performance against interframe attacks, many tests were performed, including frame drop, frame installation, and frame change. Video performance with watermark is calculated using SNR, Corelation Property, BIR etc. Peak signal-to-noise rating (PSNR) is rated to ensure video reliability. It is a quality metric used to determine corruption in embedded video in relation to video hosting. PSNR is based on MSE. The MSE is calculated by considering the difference between the estimates made by the measurement and the actual values of the estimated value. SNR is defined as a signal measurement; the power of sound effects. It is expressed in decibels. In the case

of watermarking, the rate of slight change should be considered. After all, no one wants the video size to be huge after embedding a watermark. If the conversion rate is small, we can get better video integration.

In this paper we suggest the watermarking algorithm for a fragile video that should have the following requirements:

1. Background: The embedding and removal of watermark is performed on a local domain and pixel intelligence system.
2. Insightful quality: Watermark embedding should not reduce video quality hosting.
3. Watermark: A watermark is a digital video that is repeated several times with the same size as the frame of the hosted video. This requirement is made so that we can identify interference up to the pixel level.
4. Security: For only authorized people to verify the video obtained, the watermarking algorithm should consider a security issue.
5. Location detection: algorithm has the ability to cause location detection.

V. CONCLUSION

Fragile watermarking has become an exciting topic of research. Recently digital video is much easier to convert using commercial software, so there is a need to prove the authenticity of the video content. Watermarking video soft local domain based on Arnold Cat Map presented. In this case we have used the video file as a watermark in addition to the most commonly used image file. The algorithm can detect the location of the disturbance. System performance can be analyzed using various parameters such as SNR. For future tasks, an algorithm may be developed for compressed video. Watermark embedding and extraction should be used in the transform domain.

REFERENCES

[1] A.F. Elgamal, N.A. Mosa, W.K., ElSaid, "A Fragile Video Watermarking Algorithm for Content Authentication based on Block Mean and Modulation Factor", International Journal of Computer Applications (0975 – 8887) Vol. 80 – No.4, October 2013.

[2] T. Jayamalar, V. Radha, "Survey on Digital Watermarking Techniques and Attacks watermark", International Journal of Engineering Science and Technology, Vol. 2, No. 12, pp 6963-6937, 2010.

[3] H. Zhi-yu, T. Xiang-Hong, "Integrity Authentication Scheme of Color Video Based on the Fragile Watermarking", Proc. of 2011 International Conference on Electronics, Communications and Control (ICECC).

[4] Maryam A., Mansoor R., Hamidreza A., "A novel robust scaling image watermarking scheme based on Gaussian Mixture Model" in Expert Systems with Applications 42, 2015, pp 1960–1971.

[5] Rupali D. P., Shilpa M., "Fragile Video Watermarking for Tampering Detection and Localization", Proc. of 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015.

[6] Katherine S., "A Chaotic Image Encryption", Mathematics Senior Seminar, 4901, University of Minnesota, Morris, 2009.

[7] Rinaldi M., "Algoritma Enkripsi Citra dengan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif Terhadap Bit-bit MSB", Proc. of Seminar Nasional dan Aplikasi Teknologi I