Journal of Theoretical and Applied Information Technology
15th November 2016. Vol.93. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT I-ENCRYPTED VIDEO WATERMARKING SCHEME USING ENCHANCED PCA-SVD-DWT BLOCK EMBEDDING AND EXTRACTION MODEL

[1]T.SRINIVASA RAO, [2]DR.RAJASEKHAR R KURRA
[1]Assistant Professor, Dept of CSE,Andhra Loyola Institute of Engineering & Technology, India
[2]Director and Principal, Usha Rama College of Engineering & Technology, India

E-Mail: [1]srinu_tumma@yahoo.co.in, [2]krr_it@yahoo.co.in

ABSTRACT

Due to the extensive use of video streaming applications, video content and security protection have become more important in online modern applications. Video watermarking is the process of embedding essential image blocks as copyright content in video streams. A large number of digital watermark solutions have been introduced in the literature to secure illegal modifications and video distortions techniques. Frame dropping and swamping are the major factors which affect the quality and time of watermark embedding and extraction process. Also a little change in block pixels which affects the structure and contrast comparison under similar luminance background. If we drop too many frames, the quality of the watermarked video will decrease rapidly. Recent research indicates SVD (Singular Value Decomposition), Differential expansion and DWT (Discrete wavelet transform) techniques are using as integrated model with mathematical complexity. The main objective of this proposed model is to provide compression hash based lossless data during watermark embedding and extraction process using i-Encrypted PCA-SVD-DWT model. This approach provides video authentication as well as security to the data modification. This optimized model works against data integrity checking during video watermark schemes. Experimental outputs proved that proposed secured watermarking model has high efficiency in terms of time and quality is concerned.

Keywords: *Watermark, Singular Value Decomposition(SVD), Discrete wavelet transform(DWT),Principal Component Analysis(PCA), Encryption, Decryption*

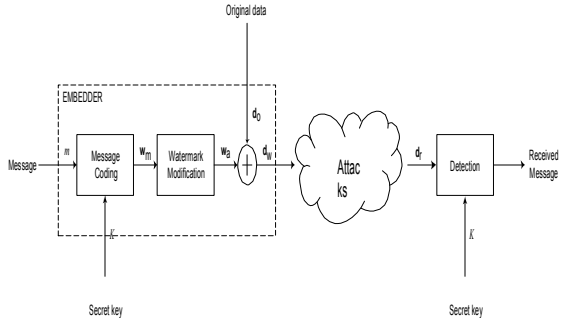
1. INTRODUCTION

Video watermarking has become one of the essential technology for enforcing digital content and copyright protection. Video watermarking techniques usually embed textual or image data in teh frequency domain. One of the most successful model is discrete wavelet transform(DWT) which is a watermarking process that represents a binary data by a set of randomized codewords. The most essential issues in video watermarking are transperancy of the watermark and the resilience of attacks.Watermarking models can be classified into three categories : transform domain models, spatial domain models and the compressed domain models[1-3].

Development of digital watermarking models for multimedia applications such as JPEG standards, and MPEG-2/4 based applications which increase in the network data communication cost and speed, which rely on digital data. These transforms are being used in several multimedia standards such as MEPG-2, MPEG-4, and JPEG2000. In addition, different watermark algorithms have been proposed using DCT and DWT. In considering the attacks on watermarks, the robustness feature of an algorithm becomes very important[4][5]. In this regard, we classify a watermark method as robust if the watermark data embedded by that algorithm in an image or any other data, cannot be damaged or removed without destroying or damaging the data itself. Therefore, an attack is successful if it can eliminate the watermark without damaging the image itself as shown in Fig 1.

Journal of Theoretical and Applied Information Technology
15th November 2016. Vol.93. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



Using the public key, anyone can encrypt messages that can only be decrypted if one possesses the private key or decryption key. A special form of public-key cryptography, called Attribute-Based Encryption, allows users to decrypt messages if their decryption key satisfies the access policy defined in the ciphertext.By using encryption, data can be protected against unauthorized access without the need of an on-line verifier authorizing data requests. The real challenge in robust digital video watermarking is achieving the desired level of robustness at a complexity that is appropriate for the target application. The robustness of a watermarking system is typically assessed by embedding a watermark into a host document, subjecting it to a number of modifications, and noting whether or not the mark is still detectable in the altered document. When determining to which modifications robustness is essential for a given application, the following categorizations may be helpful: The first describes the nature of the distortion; some are incidental, i.e., encountered during standard processing; some are intentional, i.e., introduced in an attempt to foil the watermark detector, also known as attacks; and others may fall into either category. Generally speaking, all watermarks should be resilient to incidental processing steps, as these may occur during distribution of the video. A second categorization that is useful for video watermarks is the scope of the attack; some operate on a frame-as-image basis, while others work with sequences of video frames[6][7].

Another traditional model such as video based watermarking is to combine text or image with the compression or modulation process. The combination of modulation and compression could reduce the mutual interference between the watermark embedding and extraction process especially preventing watermarking attacks.

Access structures are used to define which users have access to which resources. In the case of attribute-based authentication, attributes determine the authorization level of the user. An access structure can be regarded as a collection of sets of attributes. Each single set describes which attributes are needed to be granted access. As long as the user's attributes satisfy at least one set in the collection, the user is granted access. There are two kinds of access structures: monotonic and non-monotonic. Monotonic access structures ensure that whenever a user would be granted access based on a subset of his attributes, he will be granted access based on all his attributes. This means that no negations of attributes are possible. Nonmonotonic access structures do allow such negation of attributes. Here, the possession of an extra attribute may deny you access.

The main features of digital watermarking process are:

(i) Imperceptibility which refers to the signal similarity.

(ii) Capacity is to point of encoding or decoding per unit time in the most watermarking process.

(iii) Robustness refers to the various signal processing and its attacks in video watermarking process with effectiveness , vulnerability and safety.

Among them , inter and intra pixel dependent in the video watermarking system cant achieve same performance in all embedding and extraction models.

Video Watermarking attacks

Attack refers to the digital modification with different operations in the video watermark encoding and extraction. Due to these attacks watermarking information or original image pixel are modified with high distortion rate. The basic

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

categories of the video watermark attack as shown below:

(i) Synchronous attack: This type of attack also called distorted attack which aims to distort watermarking and video binary data of the synchromized image thus make the watermark extraction failure or embedded watermark distortion.

(ii) Normal attack: It is also known as noise or waveform attack, which is embedded watermark binary data for operation to reduce the strength of the watermark leading to the noise in the extraction process.

(iii) Interpretation attack, which detects watermarking data against the embedded algoirhtm to detect false information so as to confuse authenticity.

The main research objectives of our proposed model are:

1. Frame dropping and swaping are the major factors which affect the quality and time of watermark embedding and extraction process.
2. Also a little change in block pixels which affects the structure and contrast comparison under similar luminance background.
3. If we drop too many frames, the quality of the watermarked video will decrease rapidly.
4. Improving the security of the hidden watermark using proposed method.
5. Improving the quality of the distortion in the watermark embedded process.

This paper is organized as follows: Some related work on the video watermarking models are presented in section 2. Section 3 describes our proposed secured video watermarking model . Section 4 describes the experimental results and discussions. The last section presents our conclusion.

2. LITERATURE SURVEY

Most of the video watermarking techniques[6-8] compute the prediction value by exploiting only the similarity between the encoded pixel and its adjacent pixels, thus minimizing the watermarking efficiency of these algorithms. They obtain twelve prediction pivot values from adjacent pixels of the encoded pixel based on the model assumption -- it is easy to find out that an encoded pixel or similar to one of its neighbor pixel values in a input watermark image. The final estimated value can then be choosen from these estimated candidates by using the computed value and the original pixel intensity[8]. Fragile based watermarking techniques cover the majority of the literature works in the field of reversible watermarking models. With the term fragile, a watermarking alogorithm which embeds a block of pixels in an image that is not readable format . It presents a high visual quality, high-capacity and irreversible data encoding model for gray-scale images. This model computes the deviation of neighboring pixel values and then estimate sum of such deviations to perform a differential expansion (DE) method. In such deviation values, the embedded block can be made by the using the following parts .

(i) the original LSB and MSB values, and

(ii) JBIG compressed blocks,

(iii) computed image hash value.

In video watermarking, the watermark data can be encoded in transform domain model or spatial domain model[9].Tranform watermarking model has better performance than spatial domain model in video streaming process. Modifying the SVD of the inpute image is one of the most efficient models in spatial domain watermarking.[9] first applied the singular value decomposition based watermarking techniques of the whole frame or

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

part of it. [10] gave an random image watermarking process using SVD positional pixel value.[11] SVD and DCT are combined for video watermarking which easily affects the block and embedded image. Traditional SVD ,DCT and Hybrid SVD-DCT are dependent on fixed image sizes and are not applicable to noisy images. Our research model is secured and independent of input image size . Also traditional models are not secured against man in the middle attacks. Our research model has strong encryption model against man-in-the-middle attacks.

[12] proposed a whole image singular value decompositivon with watermarking technique and the binary data is encoded by modifying the deviation between neighbour values and this technique has good robustness against transcoding and compression but may affect moving corruption.But the main issue is how to design a distortion scheme which is robust to high capacity and transcoding good imperceptibility are always a big issues for video watermarking. To solve this issue a novel DWT model with high capacity embedded and integrity computation model has been used to improve the security in the watermarking process.

3. PROPOSED ALGORITHM

3.1. Block based Hash Algorithm:

Input: User Data Files

δ [] be the number of available processed blocks.

ψ [] be the list of processed blocks.

Output: Computed Hash Value.

Procedure:

For each block in the Image

Read binary data f,

Let N bet the number of partitions, each with bytes bits.

Divide data-file into N partitions each with bytes.

N=f.size/1024;

Data[] dt;

For each i=0 to N

Do

For each block partition p in N

Do

Let D be the block size in KB, the minimal size can be computed using

If(

$$D > \max\{\frac{\sum_{i=1}^{n}|f[i-1],p]|}{MinBlockSize}, \frac{\sum_{i=1}^{n}|f[i],p]|}{MaxBlockSize}\}$$

)

then

Assign file index f[p,i] to p.

η [i]=count(f[p,i], ψ [i]) // distributing different block data in the given dynamic patterns.

Append data η [i]'s to dynamic MD5 computation .

Else

Dt[]=f[p,i];

End if

Done

For(int k=0;k< η .length;k++)

Do

If(η [k]==empty)

Then

η [k]=count(Dt[], ψ [i])

Append data η [i]'s to dynamic MD5 computation .

Else

Continue;

Done

Done

Done

3.2.Proposed Image Encryption and Decryption algorithm:

Encryption algorithm encrypts the message using policy pattern structures. Algorithm uses three patterns with homomorphic encryption and decryption process. Additive and Multiplicative homomorphism takes two inputs and generate secure encrypted values as output. Homomorphic encryption and decryption uses $C_0, C_0^{'}$ as input.

For each block partition f[i] data

Do

For each byte j in f[i]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

M_1 =f[i][j];

M_2 = f[i+1][j];

Additive Homomorphic Encryption

$$Enc(M_1 + M_2) = p * Enc(M_1) + q * Enc(M_2);$$

Where p and q are the least square parameters.

Multiplicative Homomorphic Encryption

$$Enc(M_1.M_2) = p.q(Enc(M_1).Enc(M_2));$$

$M_1 := C_0$;

$M_2 := C_0^{'}$;

Enc(M_1):=Enc(C_0)=($C_0 + \gamma * \beta$)mod p.n

where n= $\alpha * \beta$;

Enc(M_2):=Enc($C_0^{'}$)=($C_0^{'} + \gamma * \beta$)mod q.n

where n= $\alpha * \beta$;

$Enc(M_1 + M_2)$:=Enc($C_0 + C_0^{'}$)=Enc(C_0)+En

c($C_0^{'}$);

:=($C_0 + \gamma * \beta$)mod

n+($C_0^{'} + \gamma * \beta$)mod |P| ----(1)

Enc($M_1.M_2$):=Enc($C_0.C_0^{'}$):=Enc(C_0).Enc($C_0^{'}$

);

:=($C_0 + \gamma * \beta$)mod n.

+($C_0^{'} + \gamma * \beta$)mod |P| -------(2)

Done

Cipher Text CT is publicly available to all the attribute policy holders. This CT will be decrypted only those users who has exact policy matching patterns.

Fig 1. Embedding Watermark Process using i-Encrypted PCA and DWT process(Inserted at the end of Paper)

3.3 Proposed Video Watermark Embedding Process using i-Encryption

Extract the sequence of frames from the streaming input video.

For each frame in the extracted

a. Divide the frame in to n blocks
b. For each block compute the proposed hash algorithm
    i. Repeat until no more blocks.

Done

c. Concatenate watermark image binary data and ith frame data for i-encryption process.
d. Encrypt the concatenated data using the proposed homomorphic encryption process.
e. Use PCA algorithm for feature selection of the input i-th frame. Using the SVD technique embedded the S,V,U matrices in the DWT embedding process.
f. Use dynamic pattern for embedding S,V,U matrices using watermark image.

Finally, by using the embedded frames, construct the embedded video .

Fig 2: Watermark Extraction Process in i-Decrypted SVD-DWT pattern Wise block Process(Inserted at the end of Paper)

3.4. Proposed Video Watermark Extraction Process using i-Decryption

Step 1: Input watermark embedded video.

Step 2: Extract frames from the watermark embedded video.

Step 3:For each embedded frame apply Inverse SVD for extraction process.

Step 4:Inverse Discrete wavelet transformation (DWT) technique.

Step 5:Apply Inverse SVD algorithm to extract three matrices.

Step 6:Compute the PCA components and extract S,V,U from Wframe-i.

Step 7: Finally Original Video is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

constructed after the integrity verification on the

Embedded hash and computated hash values. If both hash values are equal video is reconstructed.

Step 8: Original video is reconstructed using the extracted frames.

4.EXPERIMENTAL RESULTS

All these experiments were executed with the software configurations such as Intel(R) Core i-5, 4 GB RAM, and the operating system platform is Microsoft Windows 8 Professional. This framework requires third party libraries like joptimize, jmf and apache math.

Table 1: Comparison Of Proposed And Existing Watermark Encryption Models Using 500 Frames

Video Frames	Algorithm	Avg-Encryption Time(secs)	Avg-DecryptionTime(secs)
#500	Block DWT	15345	16474
#500	AES DWT	17455	16863
#500	RSA DWT	14755	16444
#500	AES PCA DWT	12644	11425
#500	Proposed	8934	8045

Table 1, describes the comparison of proposed secured video watermarking model with the traditional secured video watermarking models in case of 500 frames. From the table, it is observed that the average encryption and decription time of proposed is less than the existing DWT and PCA models.

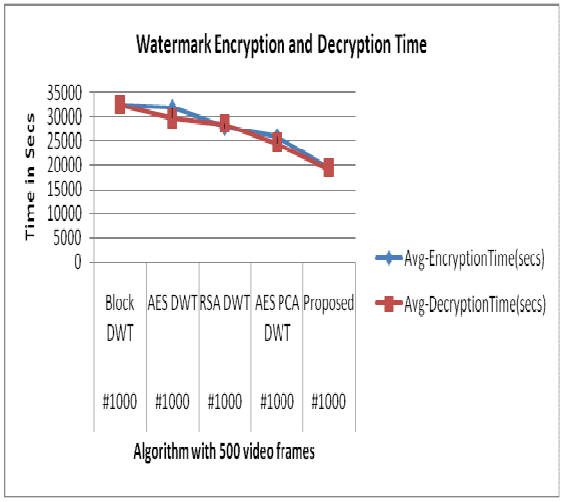


Fig 3: Comparison Of Proposed And Existing Watermark Encryption And Decryption Models Using 500 Video Frames

Figure 3, describes the comparison of proposed secured video watermarking model with the traditional secured video watermarking models in case of 500 frames. From the figure, it is observed that the average encryption and decription time of proposed is less than the existing DWT and PCA models.

Table 2: Comparisn Of Watermark Encryption And Decryption Time In Secs Using 1000 Frames

Video Frames	Algorithm	Avg-EncryptionTime(secs)	Avg-DecryptionTime(secs)
#1000	Block DWT	32454	32424
#1000	AES DWT	31844	29666
#1000	RSA DWT	27885	28555
#1000	AES PCA DWT	25844	24634
#1000	Proposed	19443	19324

Table 2, describes the comparison of proposed secured video watermarking model with the traditional secured video watermarking models in case of 1000 frames. From the table, it is observed that the average encryption and decription time of proposed is less than the existing DWT and PCA models.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

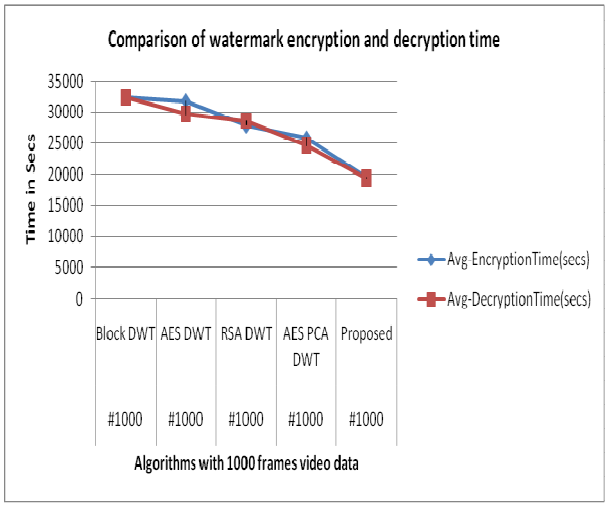


Fig 4: Comparisn Of Watermark Encryption And Decryption Time In Secs Using 1000 Frames

Figure 4, describes the comparison of proposed secured video watermarking model with the traditional secured video watermarking models in case of 500 frames. From the figure, it is observed that the average encryption and decription time of proposed is less than the existing DWT and PCA models.

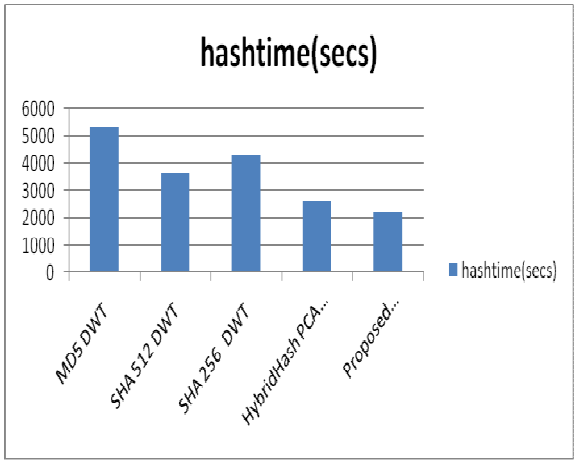


Fig 5: Comparison Of Hash Computation Using Proposed And Existing Models

Figure 5, describes the comparison of proposed block based hash model with the traditional hash algorithms. From the figure, it is observed that the average hash time of the proposed is less than the existing DWT and PCA based hash models.

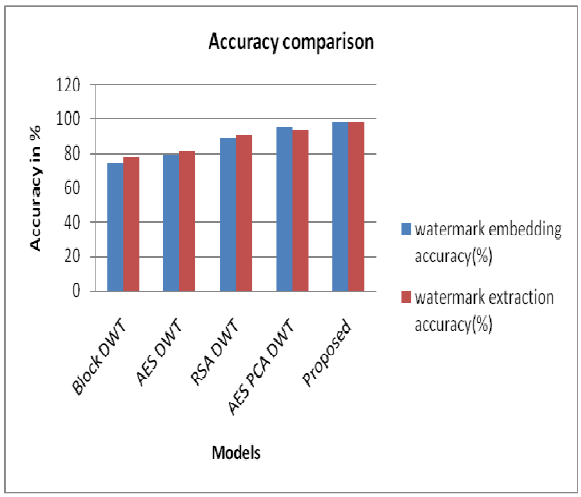


Fig 6: Accuracy Comparison Of Watermark Embedding And Extraction Process.

Figure 6, describes the accuracy comparison of proposed secured video watermarking model with the traditional video watermarking models. From the figure, it is observed that the accuracy of the proposed is higher than the existing DWT and PCA based video watermarking models.

5. CONCLUSION

Robustness of hash based watermark embedding and extraction is carried out by a large number of feature vectors. By comparing the traditional algorithms, for all the different performance metrics the proposed model has given best accuracy. This approach provides video authentication as well as security to the data modification. This optimized model works against data integrity checking during watermark extraction process. Experimental results proved that proposed secured watermarking model has high efficiency in terms of time and accuracy is concerned.

REFERENCES :

[1] W.-M. Chen, C.-J. Lai,H.-C.Wang,H.-C.Chao,C.-H.Lo, "H.264 video watermarking with secret image sharing" IET Image Process., 2011, Vol. 5, Iss. 4, pp. 349–354.

[2] Prashanth Swamy, M. Girish Chandra and B.S.Adiga, "On Incorporating Biometric Based Watermark for HD Video Using SVD and Error Correction Codes"International

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).

[3] Hui-Yu Huang, Cheng-Han Yang and Wen-Hsing Hsu," A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation" IEEE Transactions On Information Forensics And Security, Vol. 5, No. 4, December 2010, pp 625-637.

[4] Azadeh Mansouri, Ahmad Mahmoudi Aznaveh, Farah Torkamani-Azar and Fatih Kurugollu , " A Low Complexity Video Watermarking in H.264.Compressed Domain" IEEE Transactions On Information Forensics And Security,Vol. 5, No. 4, December 2010, pp 649-657.

[5] Ta Minh Thanh, Pham Thanh Hiep, Ta Minh Tam, Kohno Ryuji, "Frame-patch matching based robust video watermarking using Kaze Feature".

[6] Jantana Panyavaraporn, "Multiple Video Watermarking Algorithm based on Wavelet Transform"2013 13th International Symposium on Communications and Information Technologies (ISCIT), pp. 397-401.

[7] A.Essaouabi, F.regragui, and E.Ibnelhaj, "A Wavelet- Based Digital Watermarking for Video", International Journal of Computer Science and Information

Security, Vol. 6, No.1, pp 29-35, 2009.

[8] Kh. Manglem Singh, Th. Rupachandra Singh, O. Imocha Singh, and T. Romen Singh, "A Blind Video Watermarking Scheme based on Scene Change Detection"

[9] Saeed K. Amirgholipour and Ahmad R. Naghsh- Nilchi, "Robust Digital Image Watermarking Based on Joint DWT-DCT," International Journal of Digital Content Technology.

[10] Ali Al-Haj, ''Combined DWT-DCT digital image watermarking," Journal of Computer Science, vol. 3, no. 9, pp.740-746, 2007.

[11] S. Maity and M. Kundu, "Perceptually adaptive spread transform image watermarking scheme using hadamard transform," Information Sciences, vol. 181, no. 3, pp. 450–465, 2011.

[12] A. Agarwal, B. Paul, H. Mahmoodi, A. Datta, and K. Roy, "A process-tolerant cache architecture for improved yield in nanoscale technologies," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 13, no. 1, pp. 27–38, 2005.

Journal of Theoretical and Applied Information Technology
15th November 2016. Vol.93. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

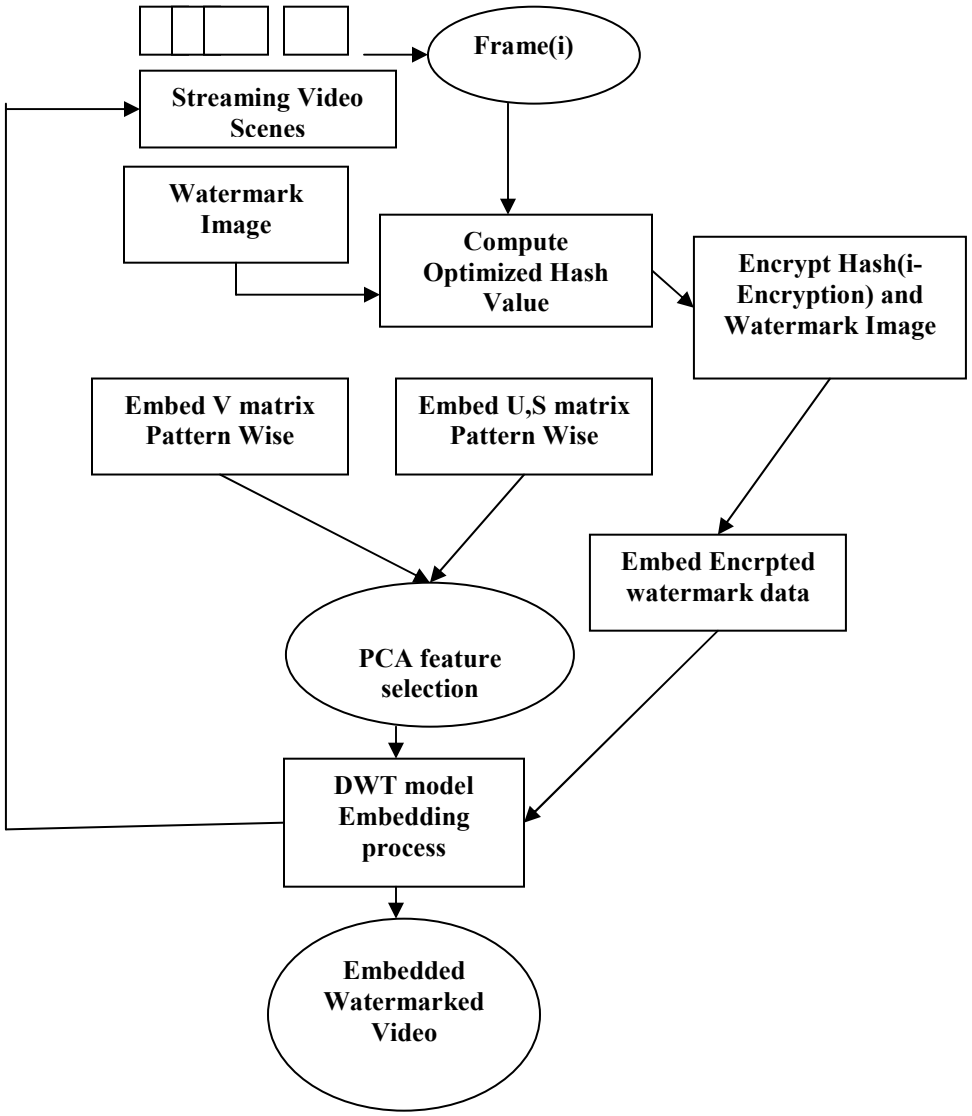


Fig 1. Embedding Watermark Process using i-Encrypted PCA and DWT process

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

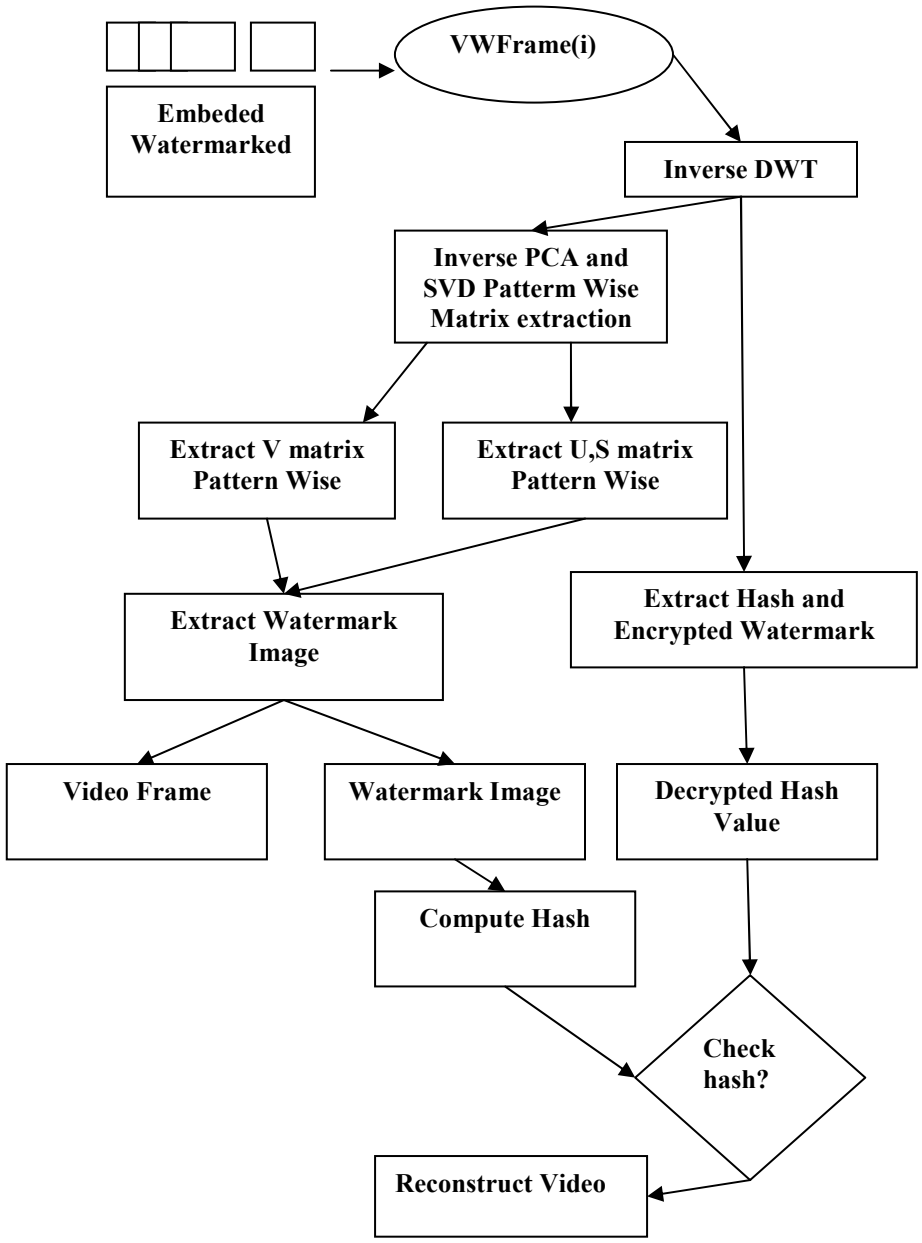


Fig 2: Watermark Extraction Process in i-Decrypted SVD-DWT pattern Wise block Process