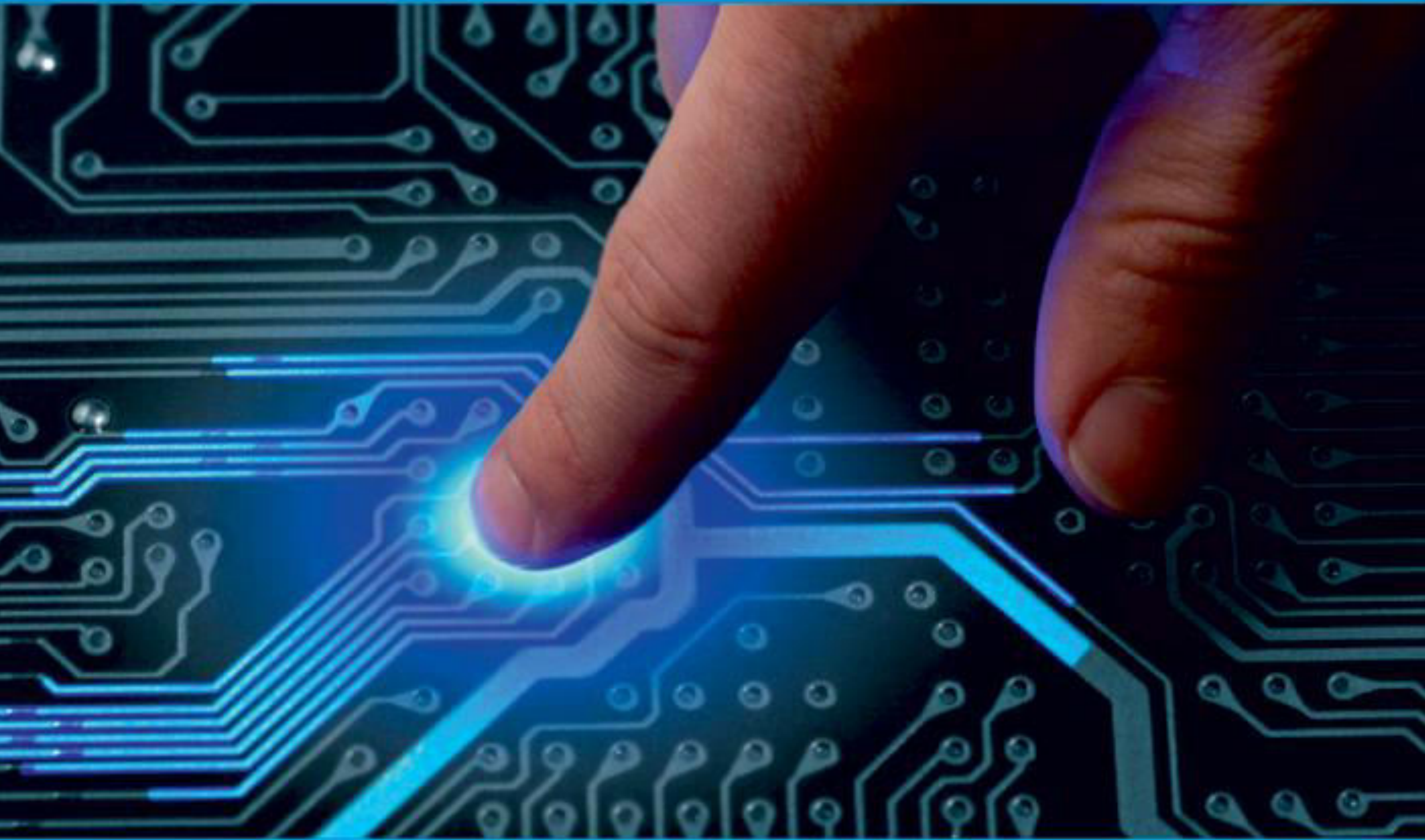
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

Implementation towards Coverless Image Steganography based on Video Watermarking

Priyadarshini S. Katore [1], Prof. Devray R. N. [2]

P.G. Student, Dept. of Computer Engineering, Vishwabharati Academy's COE, Ahmednagar, Maharashtra India[1]

Assistant Professor, Dept. of Computer Engineering, Vishwabharati Academy's COE, Ahmednagar, Maharashtra, India[2]

ABSTRACT: Data hiding should be used concealed transmissions, closed captioning, indexing, or watermarking. It is in contrast to cryptography, where the survival of the message itself is not masked, but the content is hidden. Video Watermarking is implemented in different fields such as military and Industrial applications. The 2D Barcode with a digital watermark is widely interesting research in the security field. In this paper propose a video watermarking with text data (verification message) by using the Quick Response (QR) Code technique. The QR Code is prepared to be watermarked via a robust video watermarking scheme based on the lossless video watermarking using DCT techniques messages can be sent and received securely. Traditionally, video watermark was based on hiding secret information in image files. Lately, there has been growing interest in implementing video watermarking techniques to video files. The advantage of using video files in hiding information is to be added security against hacker attacks due to the relative complexity of video compared to image files. Video-based watermark techniques are mainly classified into spatial domain and frequency domain-based methods. The main aim of video watermark is to hide information in the other wrap media so that other persons will not observe the existence of the information. This is a major distinction between this method and the other methods of secret exchange of information because, for example, in cryptography, the individuals perceive the information by considering the implied information but they will not be able to realize the information. In the reverse process check the logo and QR code for authorized ownership.

KEYWORDS: Data Hiding, Stenography, Water Marking, Cryptography

I. INTRODUCTION

Communicating and storing sensitive and confidential information has become part of day-to-day life. The digitalization of information and innovations in internet technologies has supported the exponential use of information transmission. Thus, secure transmission and storage of private information have received many researchers' attention. Actually, according to a study by the ''Ponemon Institute'' and ''IBM,'' in 2015, data breach average cost was USD 3.79 million, whereas another study by ''Juniper Research'' forecasted that by 2019, cybercrimes would cost about USD 2.1 trillion. As such, many techniques for hiding private and sensitive information in digital carriers have been developed. Hiding this information in images, text, videos, and audio is termed steganography. The method proposed in this paper depends on the following: coverless image steganography, optical mark recognition (OMR), and rule-based machine learning (RBML). So, the rest of the introduction discusses these related topics briefly.

Steganography word consists of two words of Greek origin, ''steganos'' and ''graphien,'' which, when combined, mean ''covered writing'' . Steganography is a method to secure messages during transmission by concealing them within a carrier such as an image, video, text, or audio, which results in stego media. Carriers may also include hiding information in various formats such as codes, DNA, HTML, XML, or executable files (EXE) . By using steganography, the secret message format does not change, and the actual data are maintained. The objectives are to provide end-to-end secure data communication [1], concealment of the communication existence, and personal data protection. The cover medium chosen for embedding must have two features: it should be familiar, and the modifications should be invisible to a third party. To the best of our knowledge, digital images are the most famous carrier in steganography because they contain significant amounts of redundant data and can conceal sensitive data without any visible effects. So, in image steganography, confidential information is exclusively hidden in images.

In almost all traditional image steganography methods, the payload is embedded into cover image pixels, creating modification effects. In these methods, the stego-images may be detected by any image steganalysis tool, and due to this, security cannot be guaranteed. To address this issue, a coverless data hiding concept has been proposed . Coverless data hiding was proposed to resist existing steganalysis tools, first introduced in 2015 . The main idea of this technique is to find images that contain a payload. In coverless data hiding, a mapping relationship exists between the payload and the cover image. Compared with traditional steganography, coverless steganography does not change the cover pixels, such as LSB, PVD, etc. Therefore, the security of coverless steganography methods is higher than traditional steganography methods. Coverless information hiding does not mean that a cover is not required. However, compared with traditional steganography, coverless steganography directly uses the contents of the cover itself to represent the payload. The existing coverless steganography methods can be classified into text-based and image-based methods, depending on the type of cover transmitted. For the text-based type, the current methods mainly search for the texts containing the payload according to specific rules, such as the stego-texts, then determine the location of the secret data using labels. The current image-based methods are similar to image retrieval techniques; these methods use images retrieved from the image database to represent the payload.

Paper is organized as follows. Section I gives brief introduction to the topic; Section II describes survey done to understand the problem and detect the underlying problem in system. The diagram represents the step of the process with blockchain. After transaction, how process takes place is given in Section III. Finally, Section V presents conclusion.

II. RELATED WORK

1) A Robust QR- Code Video Watermarking Scheme Based On SVD and DWT Composite Domain

Nowadays, Digital video is one of the popular multimedia data exchanged in the internet. Commercial activity on the internet and media require protection to enhance security. The 2D Barcode with a digital watermark is widely interesting research in the security field. In this paper propose a video watermarking with text data (verification message) by using the Quick Response (QR) Code technique. The QR Code is prepared to be watermarked via a robust video watermarking scheme based on the (singular value decomposition) SVD and (Discrete Wavelet Transform) DWT. In addition to that logo (or) watermark gives the authorized ownership of video document’s is an attractive algebraic transform for watermarking applications. SVD is applied to the cover I-frame. The extracted diagonal value is fused with logo (or) watermark. DWT is applied on SVD cover image and QR code image. The inverse transform on watermarked image and add the frame into video this watermarked (include logo and QR code image) the video file sends to authorized customers. In the reverse process check the logo and QR code for authorized ownership. These experimental results can achieve acceptable imperceptibility and certain robustness in video processing.

2) An Optimized Un-Compressed Video Watermarking Scheme based on SVD and DWT

In this paper, we present a novel fast and robust video watermarking scheme for RGB uncompressed AVI video sequence in discrete wavelet transform (DWT) domain using singular value decomposition (SVD). For embedding scene change detection is performed. The singular values of a binary watermark are embedded within the singular values of the LL3 sub-band coefficients of the video frames. The resultant signed video exhibits good quality. To test the robustness of the proposed algorithm six different video processing operations are performed. The high computed PSNR values indicate that the visual quality of the signed and attacked video is good. The low bit error rate and high normalized cross correlation values indicate a high correlation between the extracted and embedded watermark. Time complexity analysis shows that the proposed scheme is suitable for real time application. It is concluded that the embedding and extraction of the proposed algorithm are well optimized. The algorithm is robust and shows an improvement over other similar reported method.

3)Content -Dependent Spatio-Temporal Video Watermarking using 3 - Dimensional Discrete Cosine Transform.

In this paper we propose a content-dependent spatio-temporal watermarking scheme for digital videos. Content dependency is achieved by incorporating the hash of the video sequence into the watermark. The video sequence is treated as a 3-dimensional spatio-temporal signal for the purposes of video hash computation and watermark embedding and detection. Our experiments show that the video hash algorithm has good discriminating power and robustness against various attacks. The watermark is also shown in the experiments to have good robustness against a variety of attacks, in particular when the watermark is copied from one video sequence to another.

4)Video Watermarking Scheme Based On Robust QR-Code.
Nowadays, one of the popular multimedia data exchanged in the internet is Digital video. Protection requires in requires enhancing safety in commercial activity on the internet as well as media. Widely interesting research is the 2D Barcode with a digital watermark is in the field of security. By using the Quick Response (QR) Code technique, in this paper we recommend a video watermarking with text data. Via a robust video watermarking scheme the QR Code is prepared to be watermarked based on the SVD (singular value decomposition) and DWT (Discrete Wavelet Transform). SVD is an attractive arithmetical transform for watermarking applications. In addition to that logo (or) watermark gives the authorized ownership of video document. For the cover I-frame the SVD is applied. With logo (or) watermark there fused the extracted diagonal value. For SVD cover image and QR code image the SVD is applied.The watermarked image inverse transform and add the frame into video, to authorized customers this watermarked videofile sends. In the reverse process for authorized ownership check the logo and QR code. Acceptable imperceptibility achieved by these experimental results and in video processing there certain robustness.

5)A Watermark Technique based on SVD and DWT composite Function with QR-code.

Nowadays, due to development in digital image and internet technology common users can easily copy important data and produce illegal copies of image. So digital multimedia data exchange through internet is main idea which requires protection to enhance security, to resolve the copyright protection problem of various multimedia data and image, we propose different watermark technique used for data hiding by applying the QR Code technique. By using QR code we have propose DWT (Discrete-Wavelet-Transform), SWT (Stationary-Wavelet-Transform), SVD (singular-value decomposition) methodology for watermarking technique. The 2D barcode with a digital watermark is a widely interest research in security. The combination of DWT and SWT with SVD give better security, robustness and imperceptibility.

6)Digital Video Watermarking Using DWT-DFT Transforms and SVD Technique

In modern years there is no difficulty to make perfect copies which guide extensive unauthorized copying, which is an immense concern to the film, music, software and book publishing industries. Because of this unease over copyright issues, many technologies are developed to defend against illegal copying. Use of digital watermarks is one of these technologies. Watermarking does the embedding an ownership signal into the data directly. So that, the signal is always present with the data (image, audio, video). DWTDFT-SVD techniques are used in the proposed scheme to improve the robustness and overall computation requirements. The proposed algorithm is tested using three video sequences of different format. In this approach achieved PSNR of the original and watermarked video signal is more than 60 dB. The proposed scheme shows high robustness against several attacks.

III. METHODOLOGY

The proposed system is used in watermarking or data hiding with embedding the QR code in video. The architecture shows the cover image or video which is embedded with secret data in form of QR code , the processing consists generation of QR code and embedding same in video with which the embedded video is output. The next part remains of extraction.

Architecture:

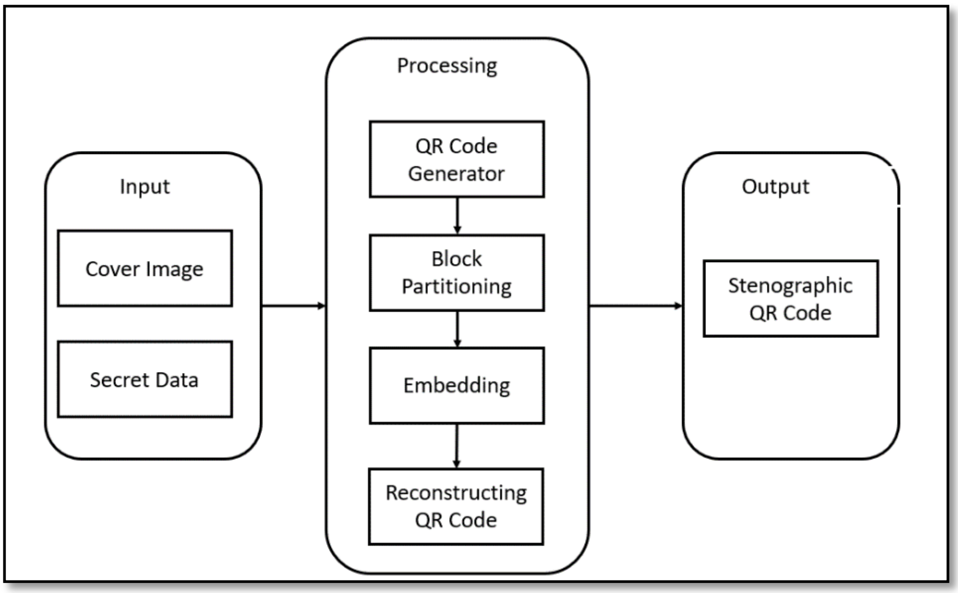


Fig.: System Architecture

Modules:

1. Input Module:
   - This module is responsible for taking in the cover image I and the secret data S that needs to be hidden.
   - It should also take in the complexity measure C and the error diffusion matrix M that will be used by the algorithm.
2. QR Code Generation Module:
   - This module is responsible for generating a QR code Q' that can store the secret data S.
   - It should use a QR code generator library to create the QR code.
3. Block Partitioning Module:
   - This module is responsible for dividing the QR code Q' and the cover image I into non-overlapping square blocks of size b x b.
   - It should ensure that the blocks in the QR code and the cover image correspond to each other.
4. Embedding Module:
   - This module is responsible for embedding the QR code data into the cover image blocks using the CADEED algorithm.
   - It should use the double-sided embedding technique to embed the bits of QR code in the LSBs of the pixels in the block.
   - It should also apply an error diffusion technique to diffuse the embedding error caused by the content-aware embedding process across neighbouring pixels.
5. QR Code Reconstruction Module:
   - This module is responsible for reconstructing a new QR code Q that includes the steganographic information from the steganographic blocks in Q'.

- It should use a QR code library to generate the new QR code Q based on the steganographic blocks.

6. Output Module:

   - This module is responsible for outputting the steganographic QR code Q.

Algorithm:

CADEED algorithm is used embedding the blocks in QR code. Content-Aware Double-Sided Embedding Error Diffusion (CADEED) is a steganographic algorithm that aims to hide secret information within digital images in a way that makes the changes to the image imperceptible to human observers. The algorithm achieves this by embedding secret data in the least significant bits (LSBs) of the cover image pixels using a content-aware embedding process and a double-sided embedding technique.

The pseud code for the same can be given as

Input:

- Cover image I
- Secret data S
- Complexity measure C
- Error diffusion matrix M

Output:

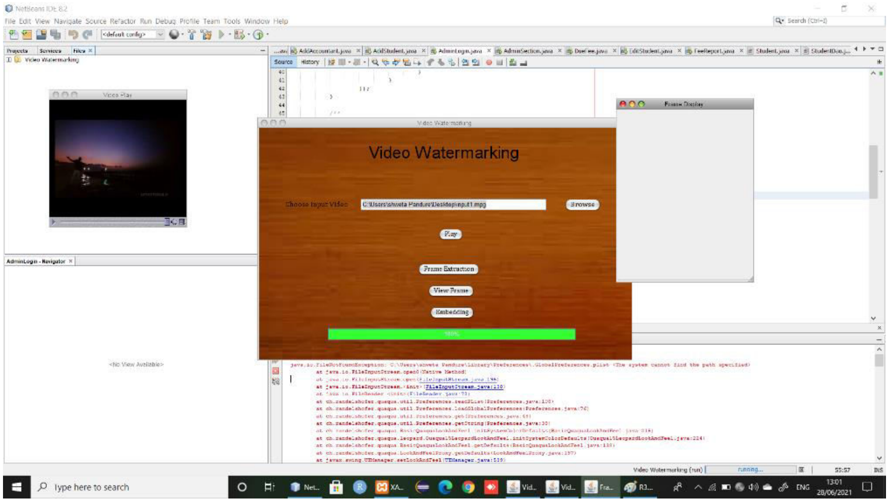
- Steganographic QR code Q

1. Generate a QR code Q' that can store the secret data S using a QR code generator library.
2. Divide the QR code Q' into non-overlapping square blocks of size b x b.
3. For each block B in Q', compute the content complexity C(B) of the pixels in the block using the complexity measure C.
4. For each block B in Q', calculate the number of bits to embed in the LSBs of the pixels in the block using a fixed embedding rate.
5. For each block B in Q', use a double-sided embedding technique to embed the bits of Q' in the LSBs of the pixels in the block. a. Compute the average value A of the pixels in B. b. For each bit to embed b_i in Q', find the pixel P with the smallest distance d_i to the target value. c. Embed b_i in both the positive and negative LSBs of P, using a bit swapping technique to ensure that the embedding does not affect the higher bits.
6. Apply an error diffusion technique, such as the Floyd-Steinberg method, to diffuse the embedding error caused by the content-aware embedding process across neighboring pixels. a. For each pixel P in Q', compute the error E(P) as the difference between the original pixel value and the embedded pixel value. b. For each pixel P in Q', apply the error diffusion matrix M to distribute the error E(P) to the neighboring pixels.
7. Generate a new QR code Q that includes the steganographic information from the steganographic blocks in Q'.
8. Output the steganographic QR code Q.

| DOI: 10.15680/IJIRCCE.2023.1106036 |

IV. RESULT AND ANALYSIS

The experimental setup for the system includes performance for watermarking with help of QR code. The following images show step wise direction for implementation of watermarking with QR code.

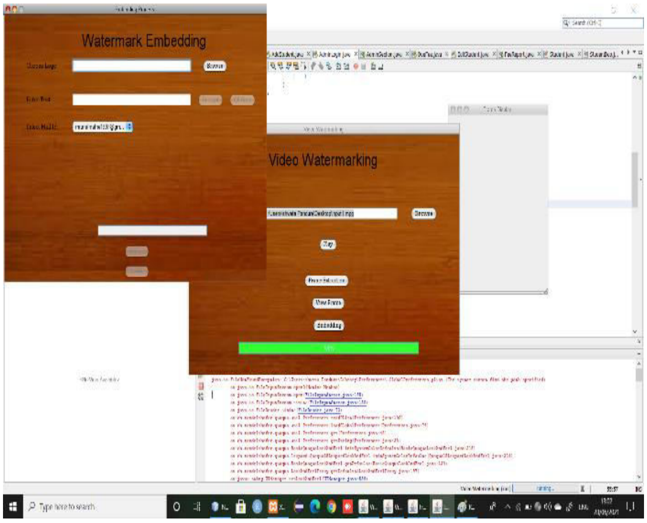


Choose Input Video: C:\Users\shweta Pandure\Desktop\input1.mpg

```
java.io.FileNotFoundException: C:\Users\shweta Pandure\Library\Preferences\.GlobalPreferences.plist (The system cannot find the path specified)
	at java.io.FileInputStream.open0(Native Method)
	at java.io.FileInputStream.open(FileInputStream.java:195)
	at java.io.FileInputStream.<init>(FileInputStream.java:138)
	at java.io.FileReader.<init>(FileReader.java:72)
	at ch.randelshofer.quaqua.util.Preferences.readPList(Preferences.java:138)
	at ch.randelshofer.quaqua.util.Preferences.loadGlobalPreferences(Preferences.java:76)
	at ch.randelshofer.quaqua.util.Preferences.get(Preferences.java:45)
	at ch.randelshofer.quaqua.util.Preferences.getString(Preferences.java:30)
	at ch.randelshofer.quaqua.BasicQuaquaLookAndFeel.initSystemColorDefaults(BasicQuaquaLookAndFeel.java:318)
	at ch.randelshofer.quaqua.leopard.Quaqua15LeopardLookAndFeel.initSystemColorDefaults(Quaqua15LeopardLookAndFeel.java:224)
	at ch.randelshofer.quaqua.BasicQuaquaLookAndFeel.getDefaults(BasicQuaquaLookAndFeel.java:138)
	at ch.randelshofer.quaqua.LookAndFeelProxy.getDefaults(LookAndFeelProxy.java:157)
	at javax.swing.UIManager.setLookAndFeel(UIManager.java:539)
```

Fig3: Cover Video for watermarking

The experimentation is carried out in two steps of embedding and extraction of secret data. Fig3 shows the cover video selected in which embedding will be done. The Fig 4 is the secret data which is converted to QR code with help of QR code generator and embedded in video. Fig 5 has generated the embedded video which can be transmitted over network.



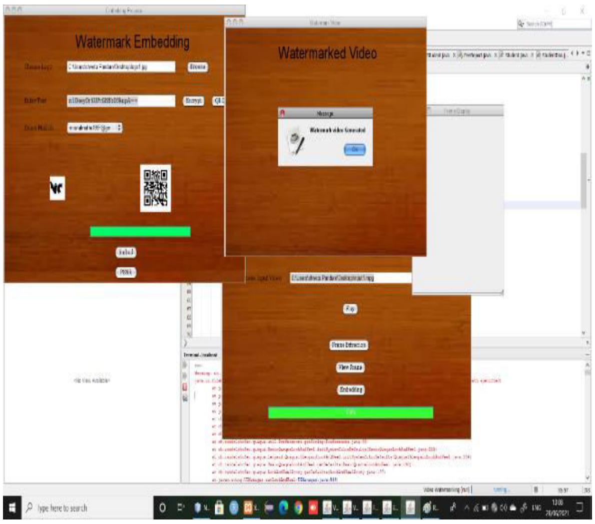


Fig4: Secret Data to embed in video generated

Fig5: QR code generated and Water marked video

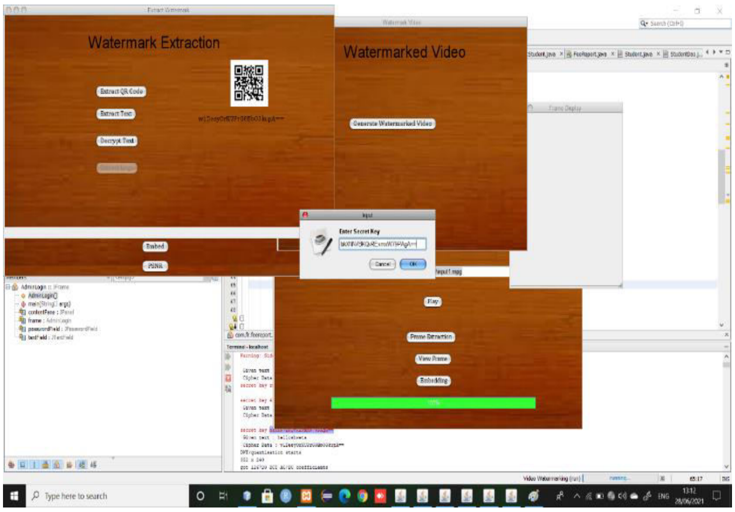


Fig6: Secret Key used for extraction

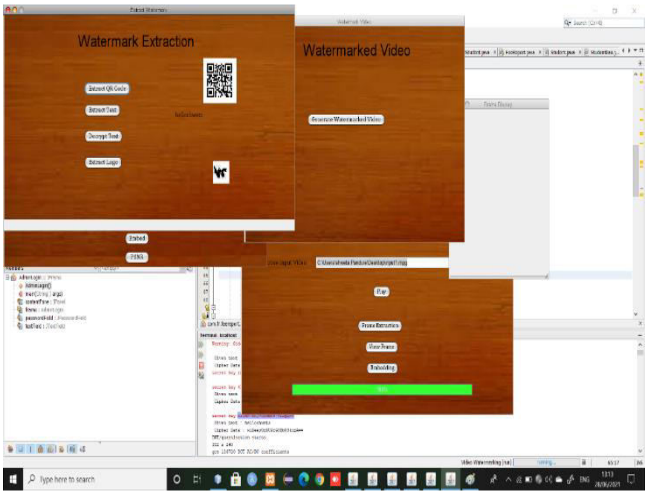


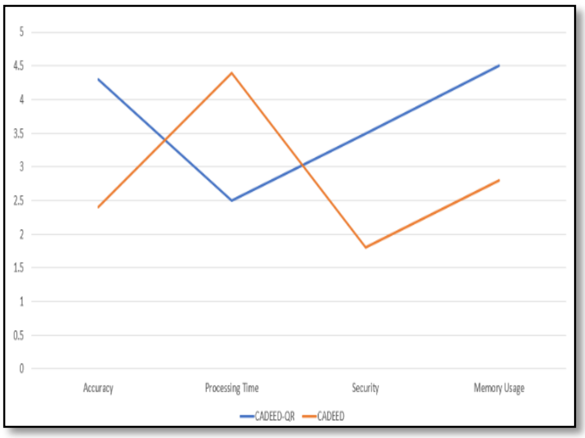
Fig7: Water Marked video extracted

The next step towards experimentation is extraction of secret data from video. Fig6 shows the setup wherein CADEED Algorithm mentioned above is used to get extracted QR code from video with help of secret key. The Fig7 shows the extracted QR code from video.

Performance analysis is performed on two perspectives of embedding the data in video and extraction of data from video. The graph gives comparison for CADEED algorithm and CADEED with QR code, the results show that that security and accuracy is increased with CADEED-QR

Table 3: Performance Analysis

	Accuracy	Processing Time
Embedding	0.849	3.5 min
Extraction	0.745	4 min



V. CONCLUSION

This method has achieved the improved imperceptibility and security watermarking. In this QR code encoding process and get excellent performances. In the first method watermark was embedded in the diagonal element. On the other hand embedding text messages in the QR code image. So, the dual process given two authentication detail. The logo is located very safely in the QR code image. This method is convenient, feasible and practically used for providing copyright protection. Experimental results show that our method can achieve acceptable certain robustness to video processing.

In our future work, we will extend our proposed system related to video compression and continue to investigate the performance of the proposed scheme for a wider range of video inputs and attacks. Furthermore, we will also investigate techniques to increase the robustness of the scheme against temporal attacks

REFERENCES

1] M.U. Celik, G. Sharma, E. Saber and A.M. Tekalp, “Hierarchical watermarking for secure image authentication with localization,” IEEE Trans. Image Process., vol. 11, no. 6, pp. 585-595, 2002.
2] E. Walia and A. Suneja, “Fragile and blind watermarking technique based on Weber’s law for medical image authentication,” IET Comp. Vision, vol. 7, no. 1, pp. 9-19, 2013.
3] C.J. Cheng, W.J. Hwang, H.Y. Zeng and Y.C. Lin, “A fragile watermarking algorithm for hologram authentication,” J. Display Tech., vol. 10, no. 4, pp. 263-271, 2014.
4] X. Cao, L. Du, X. Wei, D. Meng and X. Guo, “High capacity reversible data hiding in encrypted images by patch-level sparse representation,” IEEE Trans. Cybernetics, 2015.
5] E. Nezhadarya, Z.J. Wang and R.K. Ward, “Robust image watermarking based on multiscale gradient direction quantization,” IEEE Trans. Inf. Forensics and Security, vol. 6, no. 4, pp. 1200-1213, 2011.
6] A.V. Subramanyam, S. Emmanuel and M.S. Kankanhalli, “Robust watermarking of compressed and encrypted JPEG2000 images,” IEEE Trans. Multimedia, vol. 14, no. 3, pp. 703-716, 2012.
7] H.D. Kim, J.W. Lee, T.W. Oh and H.K. Lee, “Robust DT-CWT watermarking for DIBR 3D images,” IEEE Trans. Broadcasting, vol. 58, no. 4, pp. 533-543, 2012.
8] J. Wang, S. Lian and Y.-Q. Shi, ”Hybrid multiplicative multiwatermarking in DWT domain”, Multidimensional Systems and Signal Process., vol. 28, no. 2, pp. 617C636, 2017.
9] T. Zong, Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou and G. Beliakov, “Robust histogram shape-based method for image watermarking,” IEEE Trans. Circuits and Systems for Video Tech., vol. 25, no. 5, pp. 717-729, 2015.
10] C. Yuan, Z. Xia and X. Sun, “Coverless image steganography based on SIFT and BOF,” J. Internet Tech., vol. 18, no. 2, pp. 435-442, 2017.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.379

doi crossref

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details

www.ijircce.com