ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 5 , May 2016

Secure Remote Authentication for Wireless Networks

Shruti M Chougule., S.R.Mahadik

P.G. Student, Department of Electronics Engineering, Dr J J Magdum college of Engineering,Jaysingpur ,Maharashtra , India

Associate Professor, Department of Electronics and Telecommunication Engineering, Dr J J Magdum college of Engineering,Jaysingpur ,Maharashtra , India

ABSTRACT: In wireless communications sensitive information is frequently exchanged, requiring remote authentication. Remote authentication involves the submission of encrypted information, along with visual and audio cues (facial images/videos, etc.).This paper proposes a robust authentication mechanism based on cryptography and stegnography. Assuming that user X wants to be remotely authenticated, initially X's video object (VO) is extracted . Next, one of X's biometric signals is encrypted by XOR method . Afterwards the encrypted signal is inserted to the most significant wavelet coefficients of the VO.Finally, the Inverse Discrete Wavelet Transform (IDWT) is applied to provide the stego-object (SO).

KEYWORDS: Remote authentication, cryptography, stegnography, stego-object.

I. INTRODUCTION

In wireless communications sensitive information is frequently exchanged, requiring remote authentication Authentication is the act of confirming the truth of an attribute of a datum or entity This might involve confirming the identity of a person or software program. The two main directions in the authentication field are positive and negative authentication. Positive authentication is well-established and it is applied by the majority of existing authentication systems. In positive authentication, the passwords of all users that are authorized to access a system are stored, usually in a file. Thus the passwords space includes only users passwords and it is usually limited (according to the number of users). If crackers receive the passwords file, then their work is to recover the plaintext of a very limited number of passwords.

The proposed scheme is a positive authentication system and for security reasons elements from at least two, and preferably all three, of the following factors should be verified:

[1] The ownership factor: Something the user has (e.g. ID card, security token, cell phone etc.)
[2] The knowledge factor: Something the user knows (e.g., a password, a PIN, a pattern etc.)
[3] The inherence factor: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence, face, other biometric identifier etc.)

In order to further promote the wide spread utilization of biometric techniques to applications over error prone networks, increased security and especially robustness of the biometric data is necessary[1]. Towards this direction, proper combination of encryption and steganography can achieve this goal. In particular, cryptographic algorithms can scramble biometric signals so that they cannot be understood. In a real-world scenario, encryption can be applied to the biometric signals for increasing security[2]

In order to confront the problem of user authentication, in this paper, we propose an efficient wavelet-based steganographic method for biometric signals hiding in video objects, which focuses on optimizing the authentication rate of hidden biometric data over error prone transmissions. Interesting techniques for object-oriented data hiding have been presented [3], for example , however, most of them do not particularly consider the case of biometric data. Thus the main contributions and novelties of the proposed system are as follows. (a) It is one of the first to use video objects to hide their respective biometrics[4]. By this way "dual" authentication is accomplished, the first by visual perception of the figured person, and the second by extraction and matching of the hidden pattern. (b) Biometric signals are encrypted before hiding. The statistical properties of this novel combination are analyzed and presented. (c) A DWT-based algorithm is adapted for biometrics hiding. In contrast to most steganographic algorithms that are capacity-efficient, the proposed algorithm is very robust to several types of signal distortions. Even though it has been

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 5 , May 2016

incorporated in a limited number of watermarking schemes, its steganographic potential has not been examined. (d) Resistance of steganographic biometrics systems to signal distortions has not been sufficiently investigated in the literature, a topic that is extensively considered in this paper. By this way, the proposed scheme contributes to illustrate the perspective of encrypted biometrics authentication systems over error prone networks.

Biometrics and User Authentication-

Biometrics systems can identify users based on either physiological or behavioral characteristics. Individuals are concerned that security systems be put in place that would prevent unauthorized access to personal data, and that their identities cannot be stolen and used by other individuals. At present, biometrics technology holds a great deal of promise for doing just that, but is not without its limitations and certainly not without its critics. Biometrics is a field of technology which has been and is being used in the identification of individuals based on some physical attribute. As funding for research has permitted there has been an effort by several tech companies to develop standards for hardware and software that would be used throughout the industry in further development within this area. The purpose of this paper will be to look at the use of biometrics technology to determine how secure it might be in authenticating users, and how the users job function or role would impact the authentication

Cryptography-

Image data are frequently shared and stored in worldwide at various end to end. Images may contain highly confidential and responsive informations . Image type of data are particularly used in the area of military wing, forensic department, intelligent agencies, medicine researches, government sectors, multimedia, film division etc .During their transmission ,the data can be accessed illegally and misuse by the hackers and unauthorized user. These troubles are usually happened in the internet communication . Hence data needs high protection on consistently. Ensure high protection of data, cryptography is the suitable technique keeps the data as safe as in transfer. Main reason behind using cryptography is authentication, secrecy, non disclaimer, consistency and honesty at any instant of data transfers. Cryptography can be describe as the skill of protection file and it makes sure that only the related people to access the content .

Stegnography-

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images.

Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret . Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised.

The work in this paper is divided in two stages. 1) Transmitter Side 2)Receiver side.
Paper is organized as follows. Section II describes video object extraction using morphological operations and encryption . The flow diagram represents the step of the algorithm and Harr DWT that is given in Section III. Section IV presents experimental results.Finally, Section V presents conclusion.

II. Video Object Extraction.

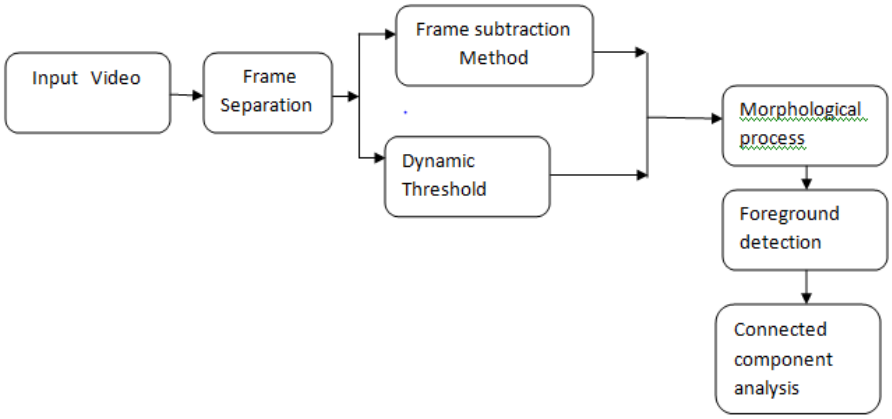
A video object extraction system for real-time applications requires the following criteria.-

1. Segmented object should conform to human perception i.e., semantically meaningful objects should be segmented.
2. Segmentation algorithm should be efficient and achieve fast speed.
3. Initialization should be simple and easy for users to operate.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 5 , May 2016



In Video Object (VO) segmentation methods, which are using mathematical morphology and perspective motion model, objects of interest should be initially outlined by human observer. From the manually specified object boundary, the correct object boundary is calculated using a morphological segmentation tool . The obtained VOP is then automatically tracked and updated in successive frames.

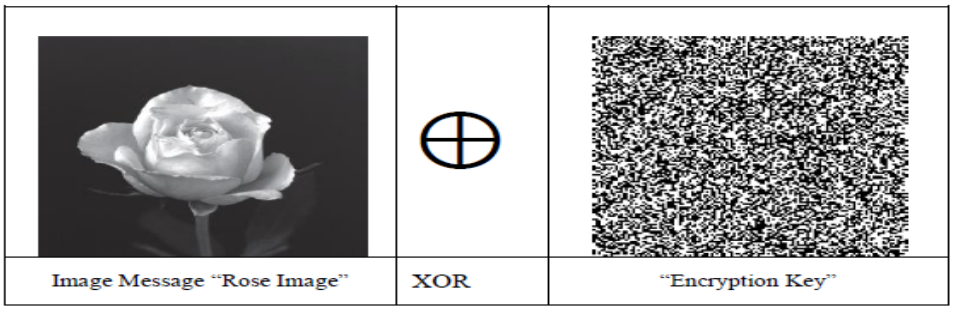
ENCRYPTION OF FINGERPRINT

Image encryption is necessary for future multimedia Internet applications. Password codes to Identify individual users will likely be replaced are biometric images of fingerprints and retinal scans in the future. However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper might duplicate or reroute the information. By encrypting these images, a degree of security can be achieved.

Encryption procedure

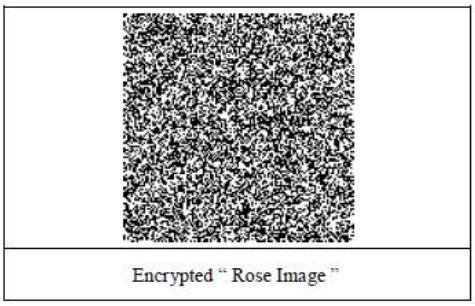
1) Input the image
2) Assign a valid key
3) Read the volume of image as matrix
4) Generate matrix of arbitrary numbers
5) Round the random values
6) Apply XOR operation of rounded values
7) Shows encrypted image effect

For Example: Below we have the image message “Rose image” embedded in a 128 by128-bit image. For a key, we have collected a 128 by 128 matrix of random bits. We will combine the two matrices using XOR.



When we apply XOR bit-by-bit to the two matrices, we get the following 128 by 128 matrix of encrypted bits.To decrypt the message, we simply take the encrypted message and compute XOR with the encryption key, bit-by-bit. This yields the original image “Rose image” message

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 5 , May 2016



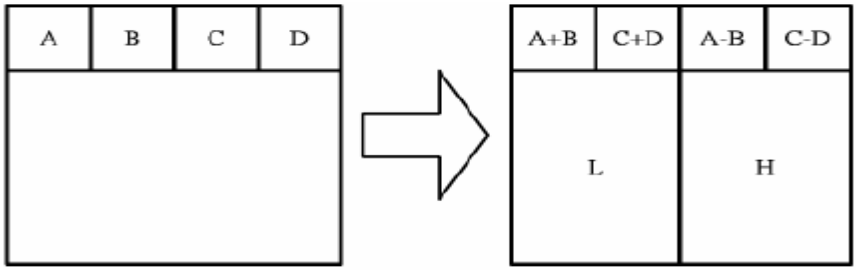
Encrypted " Rose Image "

Sometimes an image may contain text embedded on to it. Detecting and recognizing these characters can be very important, and removing these is important in the context of removing indirect advertisements, and for aesthetic reasons. Our system aims at the automatic detection of text. This is done by the algorithm. Fig. 1 shows the flow diagram of text detection algorithm.

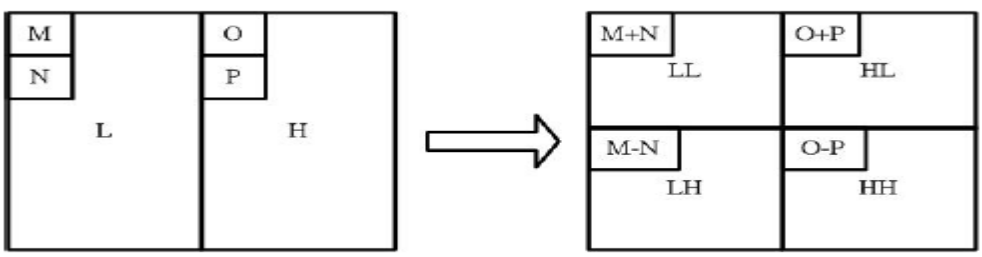
III.HAAR-DWT

The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:

Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 2. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).



Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustratedin Figure 3. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image.

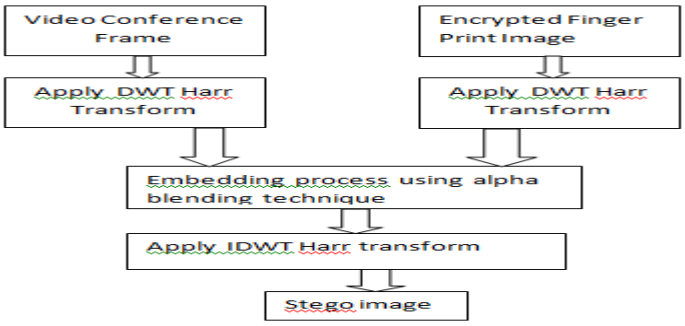


ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

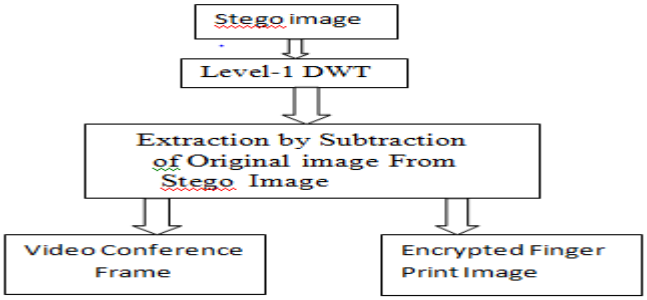
Vol. 3, Issue 5 , May 2016

FORMATION OF STEGO IMAGE



Fingerprint Embedding Process consist of decomposing Original image into 1-level sub bands using DWT which generate Four sub-bands (LL, LH, HL, HH) out of which LL (Lowest Level) has selected for Fingerprint embedding as it contain maximum energy .The Fingerprint of 128×128 is embedded into LL, Obtained image is called stego Image,

EXTRACTION OF STEGO IMAGE-



Fingerprint extraction is a process of removing fingerprint from stego image ,Inverse Discrete Wavelet Transform is used for Extraction of Watermark with Daubechies (db1)filter as shown in Figure (1).The Watermarked image is again decomposed using level 1 IDWT then DWT of image is obtained, DWT image is compared with Original image and fingerprint is extracted from stego image.

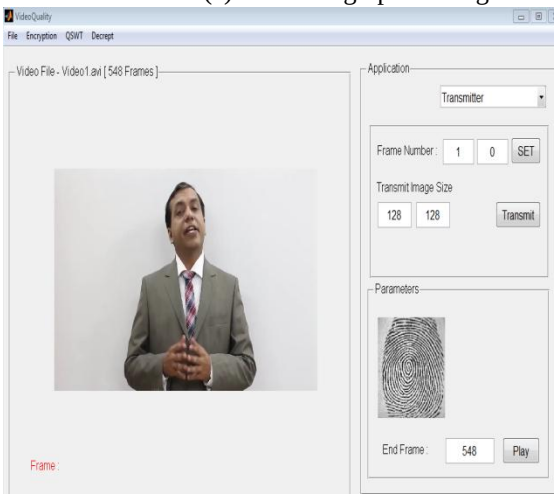
ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 5 , May 2016

IV. EXPERIMENTAL RESULTS

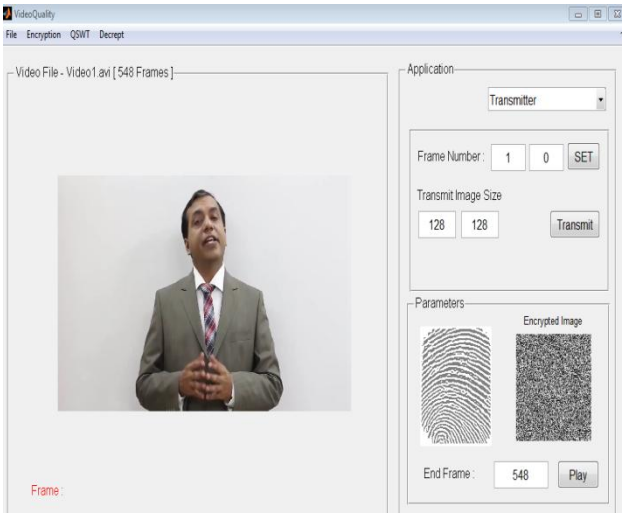
(a).Transmitter Layout-

(b).Read Video signal

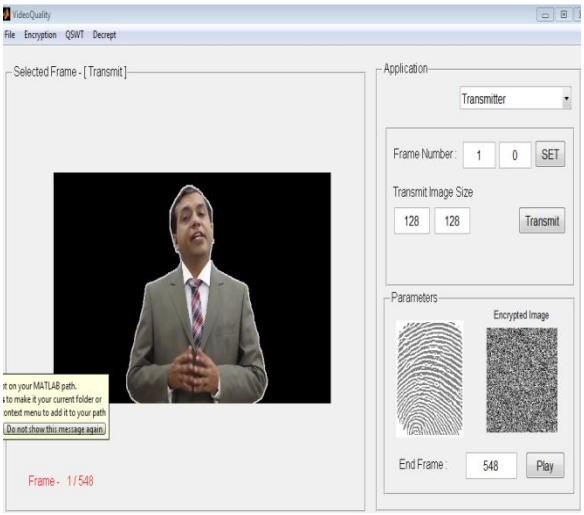
(c). Read Fingerprint Image



(d). Encryption of Fingerprint



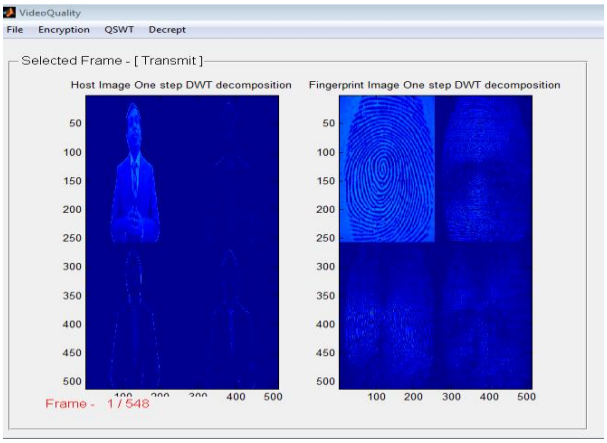
(e).Set First Frame



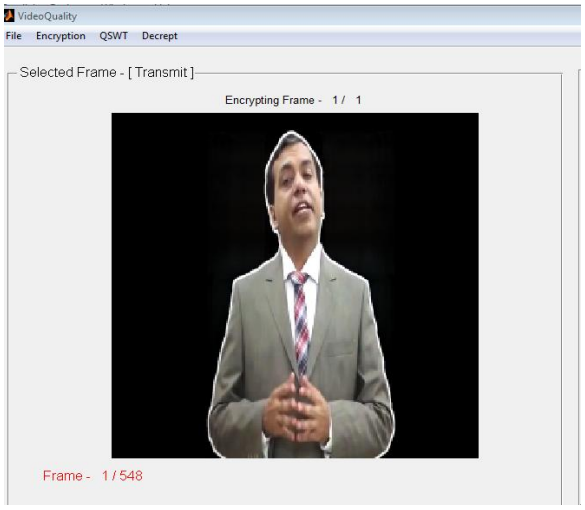
ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 5 , May 2016

(f).Extraction of host video object

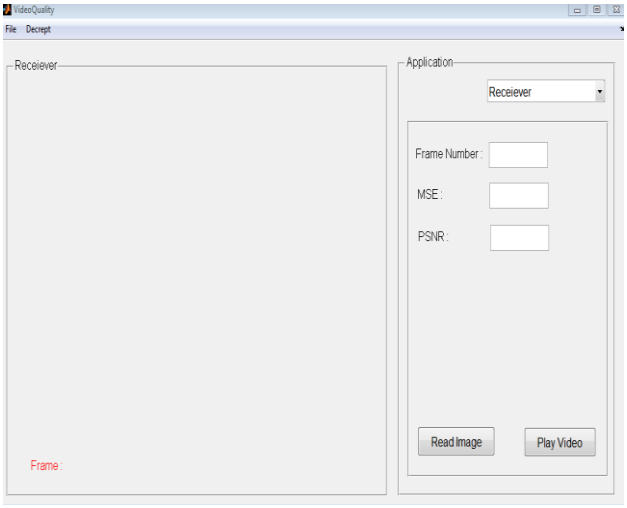
(g).Dwt of Host image and fingerprint



(h). stego image

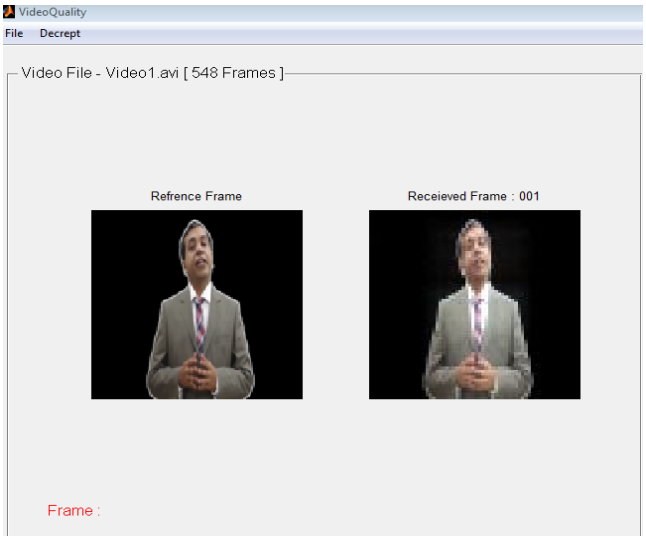


(i).Receiver layout



(j).Read the video

(k).Received Frame



ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 5 , May 2016

(l).QSWT and Decryption

V. CONCLUSION

We have implemented cryptography and stegnography with biometric authentication for wireless network. The strength of steganography amplified by combining it with cryptography. Image Steganography allowed for two parties to communicate secretly. Preposed method provides hybrid remote authentication,when both a machine and a human remotely authenticate a person

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometricrecognition," IEEE Transactions on Circuits Systems for Video Technology, vol. 14(1), pp. 4–20, 2004.
[2] D. He and D. Wang, "Robust biometrics-based authentication scheme for multi-server environment," IEEE Systems Journal, pp. 1–8, 2014
[3] M. Ramkumar and A. N. Akansu, "Capacity estimates for data hiding in compressed images," IEEE Transactions on Image Processing, vol.10(8), pp. 1252–1263, 2001.
[4] S. Li and W. Li, "Shape-adaptive discrete wavelet transforms forarbitrarily shaped visual object coding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 10(5), pp. 725–743, Aug. 2000.
[5] N. D. Doulamis, A. D. Doulamis, K. S. Ntalianis, and S. D. Kollias, "An efficient fully-unsupervised video object segmentation scheme using an adaptive neural network classifier architecture," IEEE Transactions on Neural Networks, vol. 14(3), pp. 616–630, 2003.
[6] A. M. Fard, M. R. Akbarzadeh-T, and F. Varasteh-A, "A new geneticalgorithm approach for secure jpeg steganography," in Proc. of IEEE Int'l Conference on Engineering of Intelligent Systems. IEEE, 2006.
[7] D. Kundur, Y. Zhao, and P. Campisi, "A steganographic framework for dual authentication and compression of high resolution imagery," in Proceedings of the IEEE International Symposium on Circuits and Systems, vol. 2. IEEE, 2004, pp. 1–4.
[8] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," IEEE Transactions on Industrial Electronics, vol. 48(5), pp. 875–882, 2001.