Security of Surveillance Wireless Camera Sensor Network Systems using Embedding Techniques for Authentication

Quist-Aphetsi Kester
Faculty of Informatics,
Ghana Technology University College,
Accra, Ghana
Lab-STICC (UMR CNRS 6285),
European University of Brittany,University of Brest, France

Mohammed Dolapo Asisat
Faculty of Informatics,
Ghana Technology University College,
Accra, Ghana

Ozoemena Willis Chibueze
Faculty of Informatics,
Ghana Technology University College,
Accra, Ghana

ABSTRACT
Security in today's wireless camera sensor networks is very crucial for authentication of video feeds from appropriate sources. This will ensure the safety and security of the digital video feeds as well as provide means of authenticating the video. These authentication approaches should be able to identify tamper detection. In this paper, we propose an embedding technique for authentication of video feeds obtained from wireless camera sensor networks. These approaches are able make the signals more secured and easily verifiable.

General Terms
Digital signal processing, image processing, security, multimedia, sensor networks.

Keywords
Image processing, surveillance, security, wireless sensor networks, intrusion detection systems.

1. INTRODUCTION
Security and monitory of systems and places are crucial in ensuring integrity and confidentiality of communications from different sources. With today's internet of things and sensor networks, one of the crucial needs in ensuring security in distributed usage of such applications has to do with the ability to validate the source of transmission. This ensures the integrity of the data received and authentication processes based on secured processes makes it difficult for the data to be altered without detection. This has to do specifically with transmitted data that has been protected by directly engaging features of the image data that is subject to change if tempered with.

Surveillance cameras distributed in public places are used in collecting digital video footage from the surrounding. These cameras are normally placed in public places where there are high levels of street crime in order to capture footages of such incidences. Some are also installed on traffic roads to monitor congestions as well as traffic offenders. Current surveillance systems have biometric feature extraction and analysis capabilities in identifying targeted people. These has aided in modern day policing and evidence gathering of criminal activities from monitored area. Home based video monitoring systems are also effective in maximizing security around private properties as well as providing evidential evidence of incidences. Manufacturing industries and factories nowadays engage monitory systems in observing moving parts remotely in a monitory room. These are very practical and efficient ways in monitoring moving parts that cannot be observed as humans due to the nature of the installations etc. Robots are also finding their ways into homes and monitory system and they obtain digital video data from their environments for effective processing.

Authentication and validation of signals obtained from such systems are very crucial in the investigation of incidences. In this paper, we presented an embedding technique in which we use password to embed time data as well as feature values to authenticate the source of the visual obtained. Modification of the signal may affect the stored data embedded into the stored video signal. This makes it very difficult for tampering to be done.

2. RELATED WORKS
Security in digital video or images can take form of encryption, watermarking or steganographic approaches. These approaches seek to enhance the security of digital images or video. The effective engagement of the approaches can provide a better layer of confidentiality, integrity, authentication and non- repudiation based on how they have been engaged.

2.1 Video Encryption
In the work of Changgui Shi et al they presented a fast MPEG video encryption algorithm called RVEA which encrypted selected sign bits of the DCT coefficients and motion vectors using secret key cryptography algorithms such as DES or IDEA. The RVEA features bounded computation time for any size of video frame and is robust to both plaintext and ciphertext attack. Since it adds a very small overhead to the MPEG video compression process, a software implementation is fast enough to meet the real-time requirement of MPEG video applications [1]. Vanchhit Goyal et al in their work of "A Novel Video Encryption and Decryption Scheme based on Discrete Wavelet Transform and Fractional Fourier Transform", proposed three novel algorithms for video encryption and decryption. The algorithms inserted one-level of encryption key into the existing methods. Data compression properties of the DWT (Discrete Wavelet Transform) were utilized to make the algorithm faster. The RGB channels of the frames of the video channels were compressed by these proposed methods by using two times DWT2 (2-D Discrete Wavelet Transform). The compressed

frame-channels were encrypted using 2-D FRT (The 2-D fractional Fourier transform) and random phase masks in two successive iterations. The encrypted channels were merged by two times application of IDWT2 (2-D Inverse Discrete Wavelet Transform), generating a color encrypted frame. The proposed algorithms retained the robustness of the original image encryption-decryption algorithms. Once a video frame was encrypted for a particular fractional order of FRT, decryption of this encrypted frame was only possible, when the selected fractional order for decryption is exactly the suitable for decryption [2].

They perform the encryption using the following steps:

1. Application of DWT2 twice on the primary color R, G, and B channels f (x, y) q p of original frame

2. Encoding by first CRPM.

3. First application of 2-D FRT.

4. Encoding by second CRPM.

5. Second application of 2-D FRT

6. In this last step IDWT2 was applied.

Video encryption is a computationally intensive approach in the provision of data integrity. The traditional centralized data encryption system is not enough to cope with the huge amounts of data encryption. It is difficult to have capacity to engage complex encryption approaches to accommodate the linear growth of data. Famous for allocation of resources, cloud computing becomes better choice of data processing [3]. Hence real-time video encryption technique has been proposed by some works such as using a chaotic map has proposed technique where each frame of video was encrypted using two different chaotic random phase masks in the joint transform correlator architecture. The different chaotic random phase masks were obtained either by using different iteration levels or by using different seed values of the chaotic map. The use of different chaotic random phase masks made the decryption process very complex for an unauthorized person [4]. Maniccam et al in their work presented a new method for image and video encryption. The first stage lossy video compression was based on frames difference before the encryption. The encryption methods in their work was based on the SCAN methodology which is a formal language-based two-dimensional spatial accessing methodology which can generate very large number of scanning paths or space filling curves. The image encryption was performed by SCAN-based permutation of pixels and a substitution rule which together form an iterated product cipher. The video encryption was performed by first lossy compressing adjacent frame differences and then encrypting the compressed frame differences [5]. In some cases were compression is applied, simultaneous compression and encryption method can be implementable [6].

2.2 Video Watermarking

Present day cameras sensors are employed in a distributed way to capture videos for different tasks such as surveillance. Forgery or replacement of some surveillance video clips sometimes happen with hopes to destroy evidences or obtain illegal profits. Hence authentication to prove the genuineness and integrity of the source video or trace the source of a video information leak has become a growing requirement in these small businesses. Video watermarking approaches provides an effective technology to resolve this issue. In the work of Liu, Shaohui et al, they proposed a real-time video watermarking scheme for MPEG. They in the first step exploited fast scenes segmentation to original video sequence and adaptively selects appropriate scenes to be embedded. They then engaged visual model to modulate watermark strength. Watermarks were embedded by adjusting the number of bit1in the bit streams through changing level of run-level pairs. Their experiment results showed little loss of video quality and also exhibit excellent robustness against many attacks. The watermark was directly detected in bit streams domain and real-time detection became a reality [7]. The below diagram showed the embedding of the watermark bits.

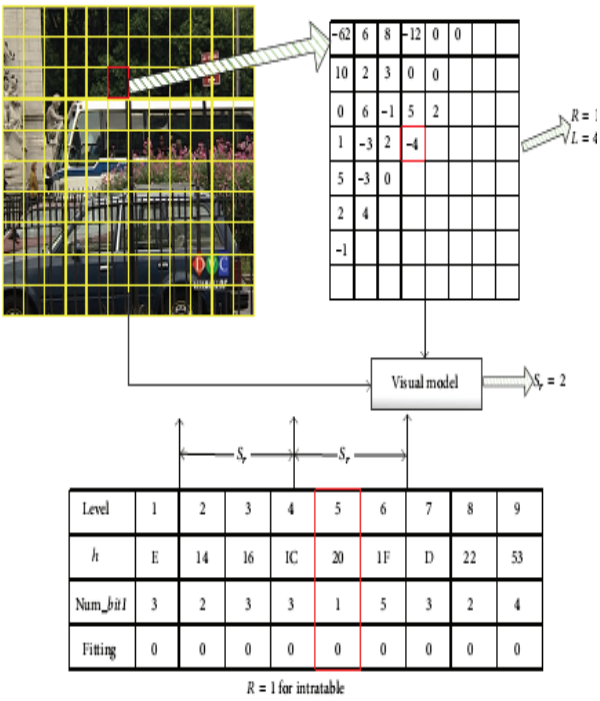

Fig 1: The embedding of watermark bits

Digital watermarking is one of the most powerful tools used in ownership and copyrights protection in digital media. In some cases a blind digital video watermarking technique can be engaged in the process so that it might not attract attention for its removal or tempering and a case is a blind watermarking technique based on a combination scheme between the Discrete Wavelet transform in (DWT) and the real Schur Decomposition. The scheme starts with applying twolevel DWT to the video scene followed by Schur decomposition in which the binary watermark bits are embedded in the resultant block upper triangular matrix. The proposed technique showed high efficiency due to the use of Schur decomposition which requires fewer computations compared to other transforms. The imperceptibility of the scheme was also very high due to the use of DWT transform; therefore, no visual distortion was noticed in the watermarked video after embedding [8]. Even though such approaches are very effective damage to the image to certain extent can make them very difficult for extraction [8]. In the work of Gaj, Sibaji, Ashish Singh Patel, and Arijit Sur et al, a compressed domain video watermarking scheme was proposed which embeds the watermark in the homogeneous moving object within a shot of video sequence to resist geometric attacks such as rotation, scaling etc. Intuitively, object based watermarking resulted in low payload and had the least impact on visual quality since the object area was generally small and highly textured. The proposed work had two main

contributions, firstly, an existing compressed domain motion coherent block detection algorithm [10] was extended to detect the moving objects within a video shot and secondly, a watermarking scheme has been proposed by embedding within the moving objects to resist RST attacks.

2.3 Video Watermarking

The use of internet with multimedia applications and files has increased tremendously over the years. The data needs to be protected from unauthorized users to prevent undesired actions. Video Steganography is a technique to hide data of any extension into a carrying Video file. The carrier file must be a video file. It is concerned with embedding information in an innocuous cover media in a secure and robust manner [11]. The work of Dixit, M. et al dealt with data security in which secret data was embedded in cover video. The methodology for creation of a stego video was defined using the Least Significant Bit (LSB) Replacement algorithm. The secret data to be hidden was replaced at the LSB positions of pixels of the carrier video frame [12]. ShengDun Hu and KinTak, U. in their work of "A Novel Video Steganography Based on Non-uniform Rectangular Partition," proposed a novel Video Steganography which hid an uncompressed secret video stream in a host video stream with almost the same size. Each frame of the secret video was Non-uniform rectangular partitioned and the partitioned codes obtained were encrypted version of the original frame. These codes were hidden in the Least 4 Significant Bits of each frames of the host video. Their algorithm could hide the same-size video in the host video without obvious distortion in the host video [13].Bhattacharyya et al proposed a novel video steganography technique for data hiding. In their approach, data hiding operations were executed entirely in the discrete integer wavelet domain. The method used Pixel Mapping Method (PMM) in order to enlarge the capacity of the hidden secret information and provide an imperceptible stego-frame/stego-video for human vision. Experimental results demonstrated that the proposed algorithm has high imperceptibility and capacity and produces satisfactory results in terms of security of the hidden data [14]. Visual steganography is a widely engaged form of steganography. It started with the process of concealing messages within the lowest bits of noisy images or sound files. The most commonly used technique is Least Significant Bit steganography (LSB steganography). But instead of traditional LSB encoding, a modified encoding technique which that transformed the video using a Lazy Lifting Wavelet transform before the application of LSB in the sub-bands of the video was proposed by Patel K et al. Their proposed approach to video steganography utilized the visual as well as the audio component. The lazy wavelet transform was applied to the visual frames, and the data was stored in the coefficients of the visual component. Results showed that the proposed technique did not affect the higher and lower ends of the frequency distribution of the signal. Moreover, it had a high payload capacity and low computational requirements [15].

3. METHODOLOGY

In our proposed approach, we acquired the live images from the source by engaging the series of video frames, and embed the data to be used for the authentication of the image into the data frames using password protection. The embedding was done in such a way that nay modification to the stored video will result in the change in frame and thereby rendering the extraction process. This process was engaged to the image make verification possible and easy also to detect tamper. The approach was based on steganographic technique. The software for the implementation was built using visual studio. The following figure represented the approaches engaged in the process.

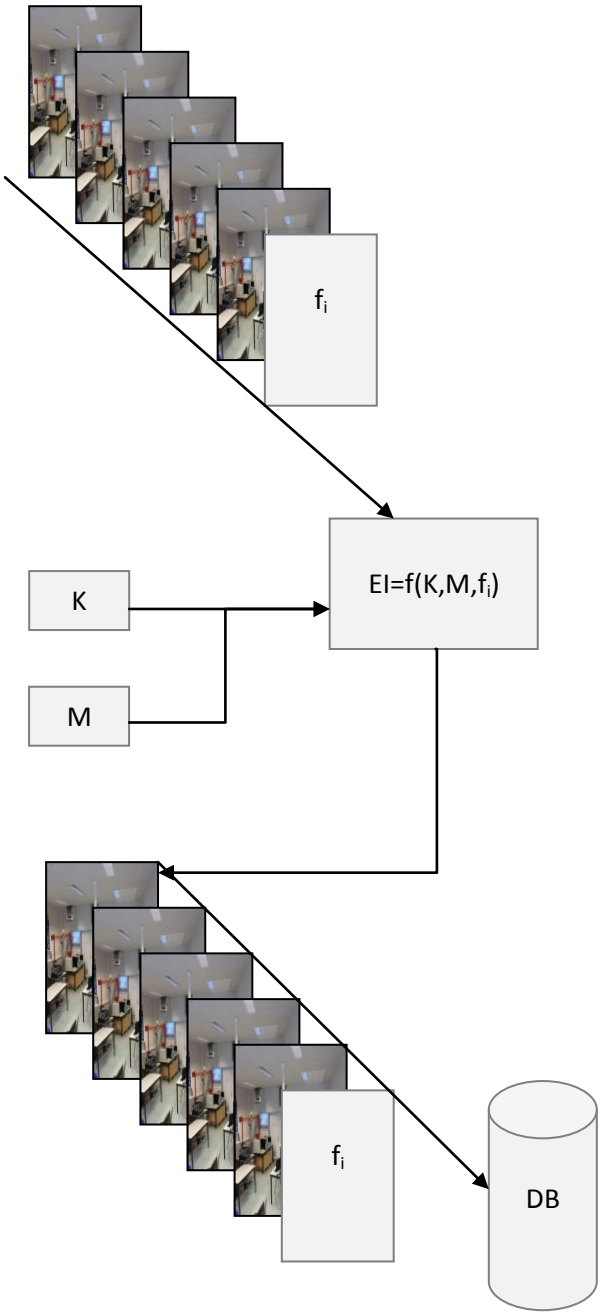

Fig 2: The Summary of the approach engaged

From the above diagram: fi represented the frames of images in the video and i=0…….n and n is the recorded last frame of the video. M is the message to be embedded and K is the secret key engaged in the embedding process.

Given a secret Key K, message defined by a set of n length of elements and the set of message M given by a set of m element, we will have them define as follows:

Let K, M ∈ Z and Z are set of integers

Let x ∈ K, M: $a \leq x \leq b$

Where a=0 and b=255

Let fi∈F and I=fi

x ∈ fi: 0 ≤ x ≤ 255

$$I = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} & . & . & . & x_{1n} \\ x_{21} & x_{22} & . & . & . & . & . & x_{2n} \\ x_{31} & . & . & . & . & . & . & x_{3n} \\ x_{41} & . & . & . & . & . & . & x_{4n} \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ x_{m1} & .x_{m2} & x_{m3} & x_{m4}. & . & . & . & x_{mn} \end{bmatrix}$$

Let I= an image=f (R, G, B)

I is a color image of m x n x 3 arrays

Size of f(R, G, B) is given by m x n

Where R, G, B ∈ I

(R o G) i j = (R) ij. (G) ij

Where r_11 = first value of R

r= [ri1] (i=1, 2… m)

x ∈ r_i1 : [a, b]= {x ∈ I: a ≤ x ≤ b}

a=0 and b=255

R= r= I (m, n, 1)

Where g_12 = first value of G

g= [gi2] (i=1, 2... m)

x ∈ g : [a, b]= {x ∈ I: a ≤ x ≤ b}

a=0 and b=255

G= g= I (m, n, 1)

And b_13 = first value of B

g= [bi3] (i=1, 2... m)

x ∈ b_i1 : [a, b]= {x ∈ I: a ≤ x ≤ b}

a=0 and b=255

B=b= I (m, n, 1

Such that R= r= I (m, n, 1)

We let M= {x1, x2,x3……xn}

and K= {x1, x2,x3……xn}

The following steps were used in the embedding process:

Let R be a pointer to which the data M will be place in fi asnd R ∈ Z.

R=f(K)

Where f(K) determines where M should be stored based on K.

Then convert the string password into an offset value.

Transform the value of M in string to Numeric equivalence within the range of a and b.

Pick intensity numeric values in the RGB component based on K.

Replace them with the values of M.

Set them pixel's color coding format.

Pass on to the next frame.

Repeat the process for all fi

The speed of the process depends on the length of M.

4. RESULT AND ANALYSIS

One of the difficulties that confront embedding data into digital video is the amount possible data that can be embedded into the host or the carrier without it being detected. The effect of this can be estimated by measuring the Mean Squared Error (MSE) and the Peak Signal to Noise Ratio (PSNR) between the cover video and the stego-video.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}||O(i,j) - S(i,j)||^2$$

$$PSNR = 10log_{10}\left(\frac{MAX^2}{MSE}\right)$$

From the given equations above,

MAX =the number of bits that represent a pixel in a frame (image). eg. MAX = 255 when pixels are presented by 8 bits.

And PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego-image should struggle for 40dB and above.

The properties of the video frames are as follows:

Table 1. Properties of video frame

Properties	**Value**
Frame width	640
Frame height	480
Data rate	1580 kbps
Total bitrate	2992 kbps
Frame rate	15 frames/second

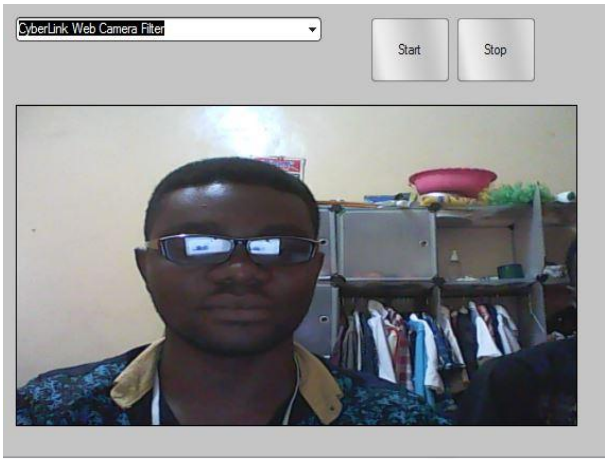

Fig 3: The developed application Interface

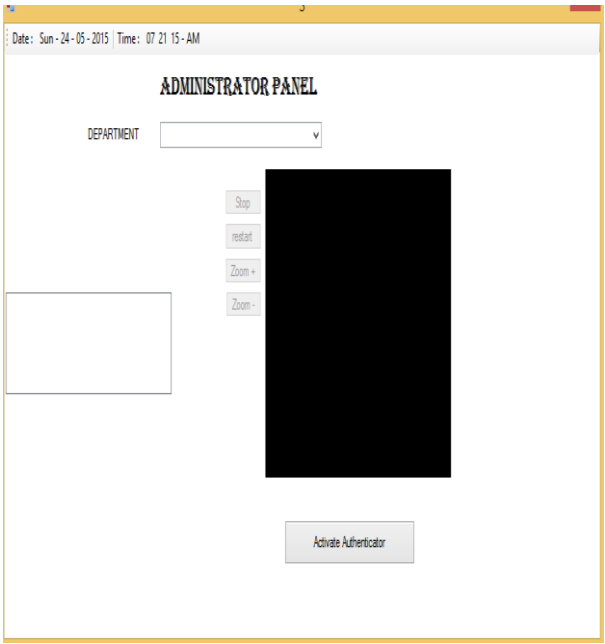

Fig 4: The the interface of the developed application in VB.net

An application was developed in VB.net and the video capturing was done using the VideoCap Pro which is an ActiveX control that allows programmers to easily integrate video capture and image processing capabilities into their software applications. The data was embedded into the frames for the authentication. The signal to noise ratio was computed after embedding the data and the following data below was computed for the first 30 frames obtained from the video signal.

Table2. Properties of video frame

Frame count	MSE x10^{-5}	SNR
1	13224	96.92
2	13208	96.92
3	13208	96.92
4	13184	96.93
5	13196	96.93
6	13138	96.95
7	13132	96.95
8	13145	96.94
9	13189	96.93
10	13159	96.94
11	13226	96.92
12	13206	96.92
13	13221	96.92
14	13136	96.95
15	13145	96.94
16	13148	96.94
17	13194	96.93
18	13208	96.92
19	13155	96.94
20	13223	96.92
21	13168	96.94
22	13198	96.93
23	13135	96.95
24	13161	96.94
25	13133	96.95
26	13139	96.95
27	13138	96.95
28	13223	96.92
29	13172	96.93
30	13136	96.95

A graph of both the mean square error and the signal to noise ration were plotted in figure 4 and figure 5 below. Since the data size to be embedded into the image did not change much in data size, the actual change in data was due to the variation in pixel intensity of the frames. This resulted in the pattern variations as shown in the graphs of the mean square error and the signal to noise ration below.

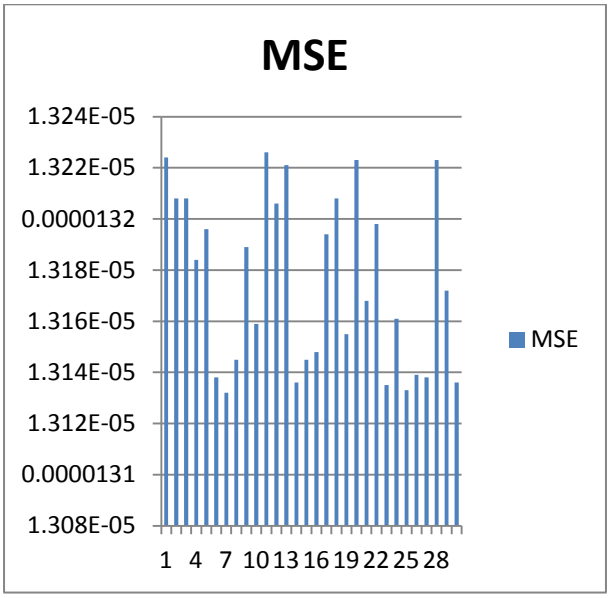

Fig 5: the graph of the mean square error of the first 30 frames

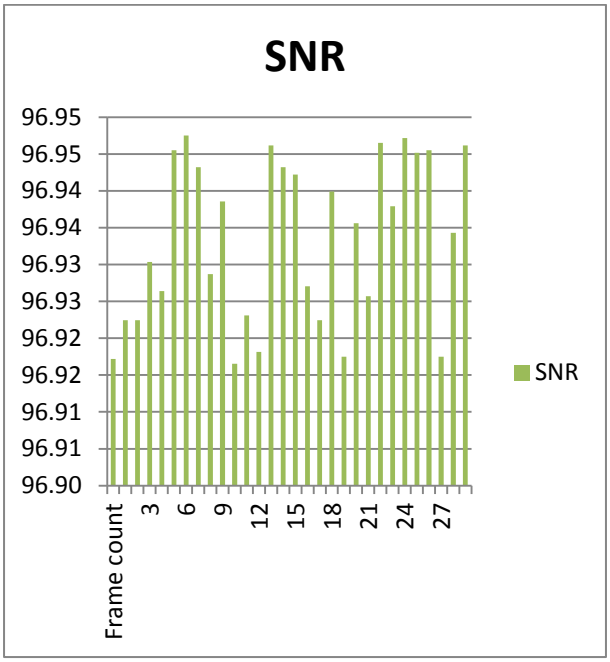

Fig 6: the graph of the signal to noise ratio of the first 30 frames

5. CONCLUSION

Experimental results showed the embedding process to be very effective and the signal to noise ratio was far above the 40 mark due to the fact that the embedding data was small and the embedding capacity too was good. The approach was a little bit faster for smaller data embedding compared to large data. There were variations for the signal ratio as well as for the mean square error each frame even though the embedding data was fixed and this was due to the fact that there were slight variations in each frame due to physical changes in humidity and intensity . but at the end the results obtained were very effective and the authentication process was very effective.

Our future works will involve the engagement of post quantum cryptographic approaches and other public key engagement in securing digital images in wireless sensor networks.

6. REFERENCES

[1] Shi, Changgui, Sheng-Yih Wang, and Bharat Bhargava. "MPEG video encryption in real-time using secret key cryptography." In in Proc. Int. Conf. Parallel and Distributed Processing Techniques and Applications. 1999.

[2] Goyal, Vanchhit, Devesh Mishra, and Ankit Agarwal. "A Novel Video Encryption and Decryption Scheme based on Discrete Wavelet Transform and Fractional Fourier Transform." International Journal of Computer Applications 111, no. 3 (2015).

[3] Moyun Li; Cheng Yang; Jiayin Tian, "Video Selective Encryption Based on Hadoop Platform," Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on , vol., no., pp.208,212, 13-14 Feb. 2015

[4] Li, Moyun, Cheng Yang, and Jiayin Tian. "Video Selective Encryption Based on Hadoop Platform." In Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on, pp. 208-212. IEEE, 2015.

[5] Maniccam, Suchindran S., and Nikolaos G. Bourbakis. "Image and video encryption using SCAN patterns." Pattern Recognition 37, no. 4 (2004): 725-737.

[6] Alfalou, A., C. Brosseau, and N. Abdallah. "Simultaneous compression and encryption of color video images." Optics Communications 338 (2015): 371-379.

[7] Liu, Shaohui, Daniel Bo-Wei Chen, Long Gong, Wen Ji, and Sanghyun Seo. "A Real-Time Video Watermarking Algorithm for Authentication of Small-Business Wireless Surveillance Networks." International Journal of Distributed Sensor Networks 501 (2015): 789536.

[8] Rajab, Lama, Tahani Al-Khatib, and Ali Al Haj. "A Blind DWT-SCHUR Based Digital Video Watermarking Technique." Journal of Software Engineering and Applications 8, no. 04 (2015): 224.

[9] Gaj, Sibaji, Ashish Singh Patel, and Arijit Sur. "Object based watermarking for H. 264/AVC video resistant to rst attacks." Multimedia Tools and Applications (2015): 1-28.

[10] Dutta T, Sur A, Nandi S (2013) Mcrd: Motion coherent region detection in h.264 compressed video. In: Multimedia and Expo (ICME), 2013 IEEE International Conference on, pp 1–6. doi:10.1109/ICME.2013.6607430

[11] Satpute, Snehal, Sunayana Shahane, Shivani Singh, and Manisha Sharma. "An Approach towards Video Steganography Using FZDH (Forbidden Zone Data Hiding)." (2015).

[12] Dixit, M.; Bhide, N.; Khankhoje, S.; Ukarande, R., "Video Steganography," Pervasive Computing (ICPC), 2015 International Conference on , vol., no., pp.1,4, 8-10 Jan. 2015

[13] ShengDun Hu; KinTak, U., "A Novel Video Steganography Based on Non-uniform Rectangular Partition," Computational Science and Engineering (CSE), 2011 IEEE 14th International Conference on , vol., no., pp.57,61, 24-26 Aug. 2011

[14] Bhattacharyya, Souvik, and Gautam Sanyal. "A novel approach of video steganography using pmm." In Wireless Networks and Computational Intelligence, pp. 644-653. Springer Berlin Heidelberg, 2012.

[15] Patel, K.; Rora, K.K.; Singh, K.; Verma, S., "Lazy Wavelet Transform Based Steganography in Video," Communication Systems and Network Technologies (CSNT), 2013 International Conference on , vol., no., pp.497,500, 6-8 April 2013