A Hybrid Cryptographic Encryption Technique for Securing Surveillance Digital Images in Mobile Urban Situation Awareness Systems

Quist-Aphetsi Kester [1,2,3], Laurent Nana [2], Anca Christine Pascu [2], Sophie Gire[2], Jojo M. Eghan[3], and Nii Narku Quaynor [3]

[1] Lab-STICC (UMR CNRS 6285), European University of Brittany, University of Brest, France

[2]Faculty of Informatics, Ghana Technology University College, Accra, Ghana

[3]Department of Computer Science and Information Technology, University of Cape Coast

ABSTRACT

With the increase in structural complexities in modern cities, many operations, be they military, police, fire service, intelligence, rescue, or other field operations, require localization services and online situation awareness to make them effective. The digital data collected from such systems are sensitive hence security concerns regarding the transmission of such digital data across secured and unsecured communication channels needs to be secured. In this paper, we proposed a hybrid cryptographic encryption technique for securing Surveillance digital images data in Mobile Urban Situation Awareness System using RSA public-key encryption cryptosystem and RGB pixel displacement. The implementation was done using MATLAB simulation software.

General Terms

Security, Cryptography, image processing, video surveillance

Keywords

Digital images, RSA, cryptography, pixel displacement

1. INTRODUCTION

We With the advent increase of technological development in urban environment, there have been increases in structural complexity and introduction of smart devices and sensors. Technologies such as unmanned transportation systems, intelligent surveillance devices, and other automated technologies are finding places and having chances of dominance in our society. Hence situational awareness of our environment is one of the ways we can effectively monitor, understand and interpret occurrences intelligently in our surroundings. These collections of information from our surroundings remotely involve both transmission and receiving of processed and unprocessed data. The privacy and security of these collected data is a concern in terms of its leakage or interception by a third party. Hence the integrity and security of the collected data needed to be protected.

In this present day century, the advancements in information technology have enabled powerful emerging capabilities, such as Urban Telepresence, wearable devices, drones etc. This allows users to experience an operational environment (e.g. an urban cityscape) via an immersive, remote browser interface. For instance the UT operators can interact in real-time with personnel and sensor assets in that environment, and can derive comprehensive shared situational awareness (SA) from a mixed reality (i.e. live-over-virtual-over-time) augmentation of the environment with supporting intelligence, including past/present/forecast information. The deployment of UT capability becomes a force multiplier for military operations as well as civilian safety, security and emergency response [1]. Also, the advancements in modern day public key cryptography [2] over the years have provided the bases for securing communications over secured and unsecured communications channels. This makes it easy for keys to be exchange for secured effective communications over protected and unprotected media of communication [3]. Public key cryptography is widely used to secure transactions over the Internet. Whilst some are now prone to known attacks, others have proven to be strong and resistive to some of these attacks [4].

This paper proposed a hybrid cryptographic encryption technique for securing Surveillance digital images data in Mobile Urban Situation Awareness System using RSA public-key encryption cryptosystem and RGB pixel displacement. The cryptographic encryption technique made use of both RSA public key-exchange algorithm and pixel displacement cryptographic encryption techniques in securing the digital images. The paper has the following structure: section 2 related works, section 3 Methodology, section 4 results and analysis, and section 5 concluded the paper.

2. RELATED WORKS

The exchange of multimedia data over adhoc networks, mobile telecommunication networks, self organizing networks, urban surveillance networks, the internet and other forms of shared networks have seen several forms of attacks and abuse of information such as unauthorized access, illegal usage, disruption, alteration [5]. This wide spread use of digital media over such communication media have increased as applications and systems evolved over the years [6]. Security concerns of such data transmission and storage has been a major concern of both the transmitters and receivers. Securing critical cyber and physical infrastructures as well as their underlying computing and communication architectures and systems is very crucial [7].

Many operations, be they military, police, rescue, or other field operations, require localization services and online situation awareness to make them effective [8]. Mobile Urban Situation Awareness Systems (MUSAS) transmit intelligence information in various formats. Digital image forms part of the most crucial forms of transmission. And some of these digital image data transmitted are sensitive data which needed to be secured from adversaries. Below are visual images from MUSAS.

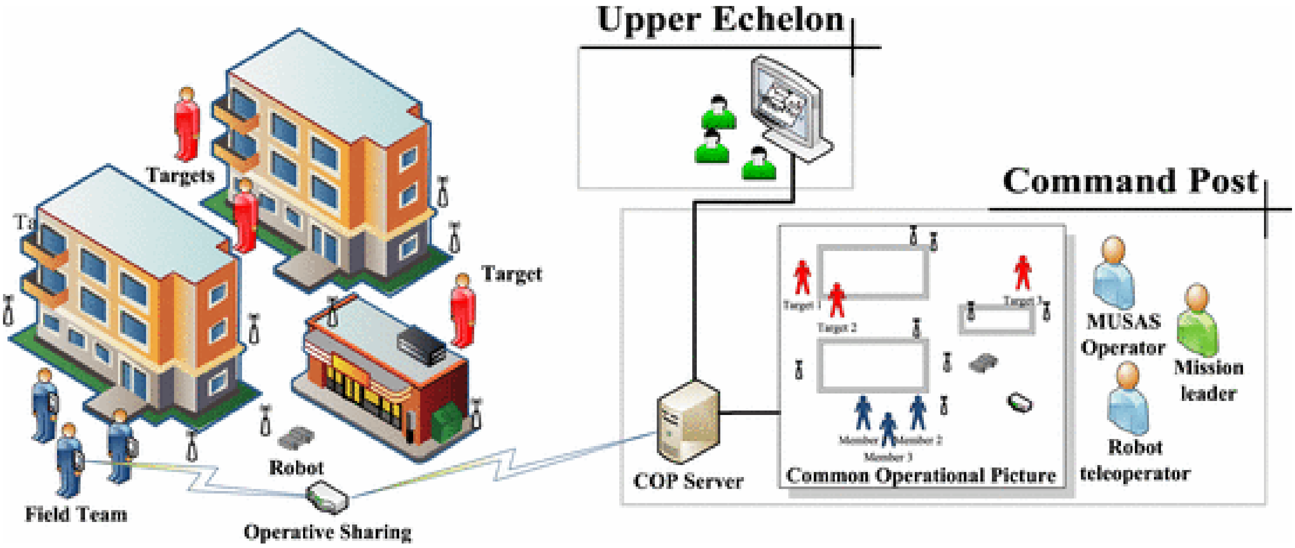

Fig 1: General use case example for the MUSAS and entities involved.

Fig 2: The mobile robot unit used for exploring, mapping and nodelocalization in the MUSAS

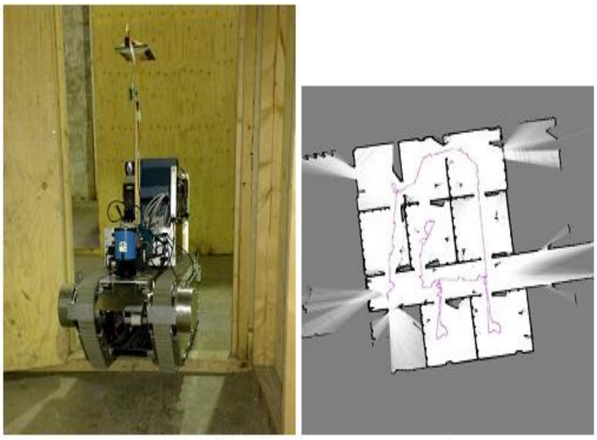

Fig 3: The robot in the test environment and An example map from the test scenario.

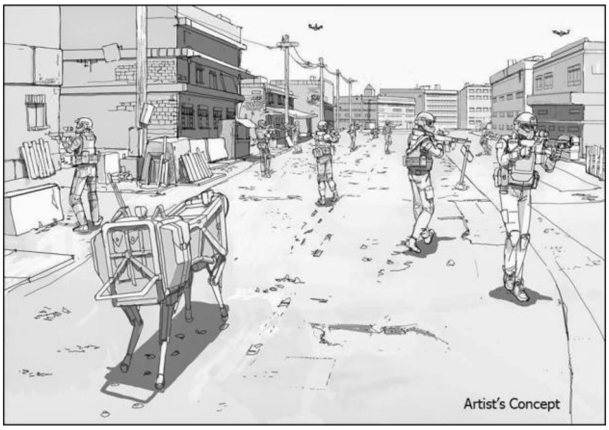

Fig 4: A depiction of DARPA Development of squad level robotics and sensing technology for urban warfare and complex environments [21].

The security of visuals obtained from these devices is very crucial for the successful executions of missions involving the engagement of them in an operation and the security over the LAN alone will not be enough provide an advantage for an operational team hence data security is needed to provide that.. A compromise situation of the transmitted video image can lead to the understanding of the position, payloads, speed, visuals, coordinates, etc of these engaged robots and these provides a positive advantage for the adversary engaged in the mission. A typical example is the capture of the “beast of Kandahar” the US drone by the Iranian force after some of the visuals during the afghan war can easily been captured by their adversaries. [22]

There have been some works done in image cryptography in securing of digital images. Musheer Ahmad and Tanvir Ahmad in their work proposed an efficient encryption method to secure the multimedia colour imagery. Complex dynamic responses of multiple high-order chaotic systems were utilized to carry out image pixels shuffling and diffusion processes under the control of secret key. The pixels diffusion was done by randomly picking the actual encryption keys out of nine hybridised keys that were extracted from complex sequences of Chen, Rossler and Chua chaotic systems. The shuffling and diffusion processes made plain-image information dependent to resist the potential chosen-plaintext, chosen-ciphertext and known-plaintext attacks [9]. He, Jun, Jun Zheng, Zhi-bin Li and Hai-feng Qian, in proposed a stream color image cryptography based on spatiotemporal chaos system. One-way coupled map lattices (OCML) were used to generate pseudorandom sequences and then used to encrypt image pixels one by one. By iterating randomly chosen chaotic maps from a set of chaotic maps for certain times, the generated pseudorandom sequences obtained high initial-value sensitivity and good randomness. The initial conditions of chaotic maps and parameters of the algorithm were generated by a 128-bit external key. Their results showed that their scheme was efficient and useful for the security of communication system [10]. Ming Sun Fu and Au, O.C. in their paper, discussed the use of both halftone watermarking and visual cryptography involvement in image hiding. They then proposed a joint visual-cryptography and watermarking (JVW) algorithm that has the merits of both visual cryptography and watermarking [11]. ShunDa Lin, in his paper proposed a new method of image transmission and cryptography on the basis of Mobius transformation. Based on the Mobius transformation, the method of modulation and demodulation in Chen-Mobius communication system, which was quite different from the traditional one, was applied in the image transmission and cryptography. In achieving such a processing, the Chen-Mobius inverse transformed functions act as the “modulation” waveforms and the receiving end is coherently “demodulated” by the often-used digital waveforms. From his results, it was established that his new applications had excellent performances that the digital image signals can be restored from intense noise and encrypted ones [12]. Singh, T.R., Singh, K.M., and Roy, S., proposed a robust video watermarking scheme based on visual cryptography. They used different parts of a single watermark as different scenes of a video for generation of the owner's share from the original video based on the frame mean in same scene and the binary watermark, and generation of the identification share based on the frame mean of probably attacked video [13]. In securing biometric data in a form of images collected from biometric devices and surveillance devices, Kester, Quist-Aphetsi, et al, proposed a hybrid encryption technique for securing biometric image data based on Feistel Network and visual cryptography [14]. Cryptography an a core part of securing data adopts technique to keep secret communications safe in order to avoid unauthorized access by making use of encryption methods such as DES, RSA etc... Chaotic approaches in encryption involves shifting the positions and changing the pixel intensity values of image by combining simultaneously to ensure a high level of security and this technique was proposed by Dongming Chen. In the work, they engaged Arnold cat map to permute the positions of the image pixels in the spatial domain. They further employed another chaotic logistic map to substitute the relationship between the ciphered image and the original image. An external 128 bit secret key was again employed and was further modified after encrypting each pixel of the original image to make the encryption more robust against attacks. At the end, sensitivity analysis of key space and statistical analysis of several experimental results were feasible [15].

The engagement of hybrid approaches in cryptography has proven to be a more convenient approach in securing data communications. [16] Proposed a system that provided the best approach for Least Significant Bit (LSB) based steganography using Genetic Algorithm (GA) along with Visual Cryptography (VC). The Original message was converted into cipher text by using RSA and then hidden into the LSB of original image. This has enhanced secure algorithm which used both Genetic Algorithm and Visual Cryptography to ensure improved security and reliability. Bansod, S.P., Mane, V.M. and Ragha, L.R., in their paper proposed hybrid cryptographic techniques based on DES and RSA algorithms to achieve data encryption and compression technique to store large amount of data. A combination of both provided a more secured control. The suggested algorithm was modified BPCS (Bit Plane Complexity Segmentation) steganography technique that can replace all the “noise-like” regions in all the bit-planes of the cover image with secret data without deteriorating the image quality [17].

3. METHODOLOGY

Asymmetric or Public key encryption is an encryption method where a message encrypted with a recipient's public key cannot be decrypted by anyone except the possessor of the matching private key, presumably, the owner of that key and the person associated with the public key used. This is used for confidentiality. [18]. Typical examples of asymmetric encryption algorithms are Rivest Shamir Adleman (RSA), Diffie-Hellman key exchange protocol and Digital Signature Standard (DSS), which incorporates the Digital Signature Algorithm (DSA). Modern day cryptography entails complex and advance mathematical algorithm are applied to encryption of text and cryptographic techniques for image encryption are usually based on the RGB pixel displacement where pixel of images are shuffled to obtained a cipher image [19].In This paper, we proposed a hybrid cryptographic encryption method that engaged both a public key exchange protocol and a pixel displacement encryption technique for securing digital images from digital image systems.

A symmetric secret encryption key was generated from the plain image and combined with a randomly chosen message. They were both used to encrypt the plain image. The plain image to be encrypted was then encrypted based on pixel displacement algorithm. The symmetric key was then encrypted using the RSA public key cryptography and then sent to the receiver as a ciphered message to be used to decrypt the ciphered image. At the end of the encryption and the decryption process, there was no pixel loss and the quality of the plain image remained unchanged after the decryption process. The proposed technique was implemented on nxm size of images and it proved to be very effective at the end. The implementation was done using MATLAB.

Figure below showed the summary of the image cryptographic approach engaged in the ciphering and the deciphering process of the digital image. Where PI is the plain image and CI is the ciphered image.

.

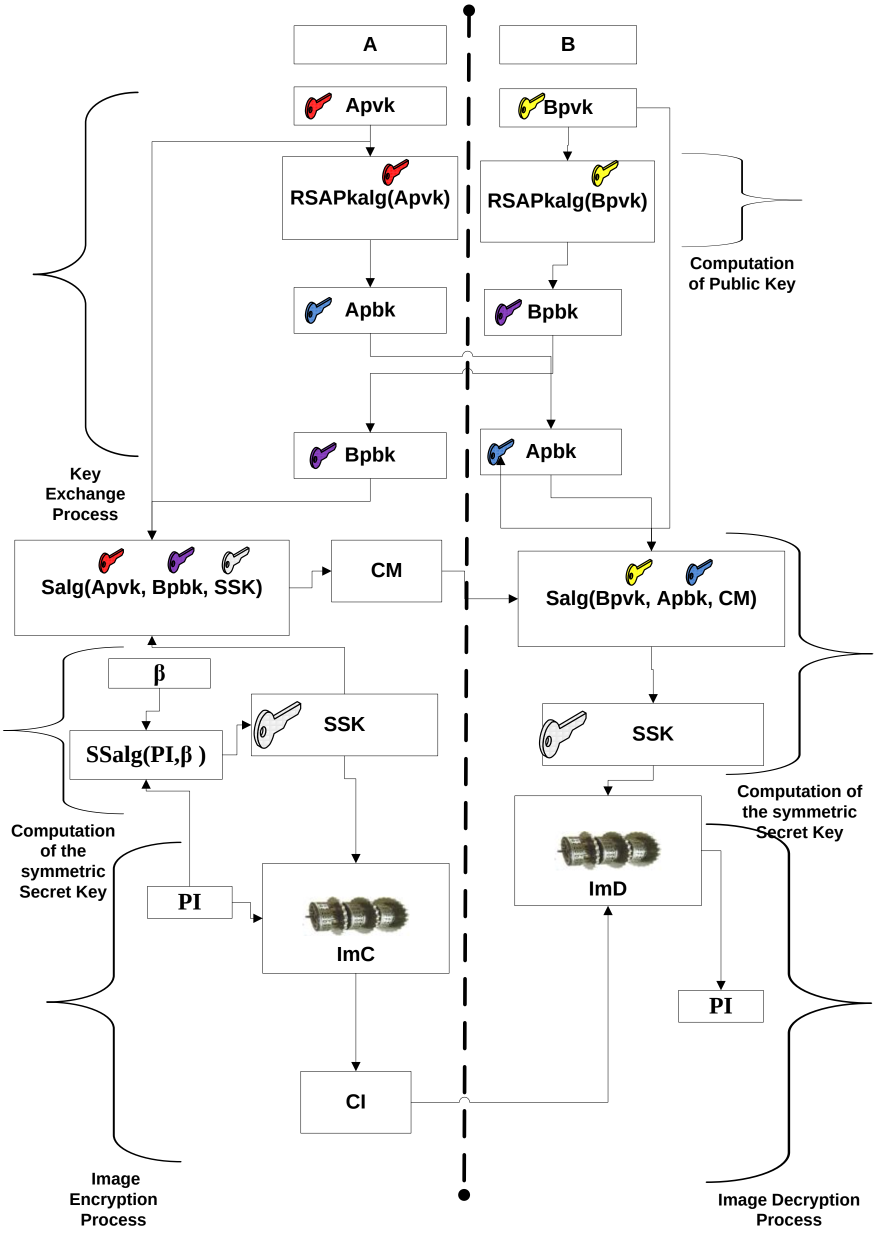

Fig 5: If necessary, the images can be extended both columns

From the diagram above,
Where PI is the plain image and CI is the ciphered image.
A = the first party being engaged in a key exchange process with B.
B= the second party being engaged in a key exchange process with A.
Apvk = the randomly chosen private key by party A.
Bpvk = the randomly chosen private key by party B.
RSAPkalg(Apvk)= the function RSAPkalg() that operates on Apvk to produce Apkb.
RSAPkalg(Bpvk)= the function RSAPkalg() that operates on Bpvk to produce Bpkb.
Apkb=the public key of party A.
Bpkb=the public key of party B.
Salg(Apvk, Bpkb, SSK) = the function Salg() that operates on Apvk, Bpkb and SSK to produce the ciphered message, CM.
Salg(Bpvk, Apkb, CM) = the function Salg() that operates on Bpvk, Apkb and CM to produce the symmetric secret key SSK.
SSK = the symmetric secret key for both party A and B.
ImC = the algorithm for encryption of the plain image.
ImD = the algorithm for the image decryption
SSalg(PI,β) = the algorithm used produce SSK.
.

3.1 The mathematical explanation of the algorithm

Please

The explanation of the processes engaged in the encryption and the decryption process is discussed bellow.

3.2 The RSA Algorithm

A Key Generation Algorithm, Digital signing and Signature verification [20].

Choose two very large random prime integers: p and q

Compute n and φ(n):

$$n = pq \text{ and } \varphi(n) = (p-1)(q-1) \qquad \textbf{(1)}$$

Choose an integer e, 1 < e < φ(n) such that:

$$\gcd(e, \varphi(n)) = 1) \qquad \textbf{(2)}$$

where gcd means greatest common denominator
Compute d, 1 < d < φ(n) such that:

$$ed \equiv 1 \ (\mathrm{mod}\ \varphi(n)) \qquad \textbf{(3)}$$

the public key is (n, e) and the private key is (n, d)
the values of p, q and φ(n) are private
e is the public or encryption exponent
d is the private or decryption exponent
The ciphertext C is found by the equation

$$'C = M^{e} \bmod n' \qquad \textbf{(4)}$$

where M is the original message.
The message M can be found form the cyphertext C by the equation

$$'M = C^{d} \bmod n' \qquad \textbf{(5)}$$

In order to sign a message the sender does the following:
Produces a hash value of the message
Uses his/her private key (n, d) to compute the signature

$$S = M^{d} \bmod n \qquad \textbf{(6)}$$

Sends the signature S to the recipient
The recipient does the following in order to verify the message:
Uses the senders public key (n, e) to compute the hash value

$$V = S^{e} \bmod n \qquad \textbf{(7)}$$

Extracts the hash value from the message
If both hash values are identical then the signature is valid

3.3 The image encryption process

a) Import data from image and create an image graphics object by interpreting each element in a matrix.
b) Get the size of r as [c, p]
c) Get the Entropy of the plain Image
d) Get the mean of the plain Image
e) Compute the shared secret from the image
f) Engage SK for g) to q) using secret key value
g) Extract the red component as ‘r’
h) Extract the green component as ‘g’
i) Extract the blue component as ‘b’
j) Let r =Transpose of r
k) Let g =Transpose of g
l) Let b =Transpose of b
m) Reshape r into (r, c, p)
n) Reshape g into (g, c, and p)
o) Reshape b into (b, c, and p)
p) Concatenate the arrays r, g, b into the same dimension of ‘r’ or ‘g’ or ‘b’ of the original image.

Finally the data will be converted into an image format to get the encrypted image.

4. RESULTS AND ANALYSIS

The β was computed form the image based on features that will remained unchanged for both the ciphered image and plain image.

Let the set of bits positions in X be x: x∈ X and X→ x: x=xi = [x0, x1, x2, x3… xn] and x ∈ I where I is a positive integer.

$$\Delta = \sum_{k=1}^{n} \Psi_k \qquad \textbf{(8)}$$

Where Ψ_k is the decimal value of x_i

$$\beta = [(c \times p) + |(\delta \times 103)| + |(gm . \textstyle\sum ni|] \bmod p \qquad \textbf{(9)}$$

$$gm = \left(\frac{1}{n}\right) \text{ and } \textstyle\sum ni = xi \qquad \textbf{(10)}$$

$$SSK = (\beta . \Delta) \bmod p \qquad \textbf{(11)}$$

Where p∈ I, δ= Entropy of image
ε = Gray value of an input image (0-255).
Ψ (η) = Probability of the occurrence of symbol η
gm is the arithmetic mean for all the pixels in the image

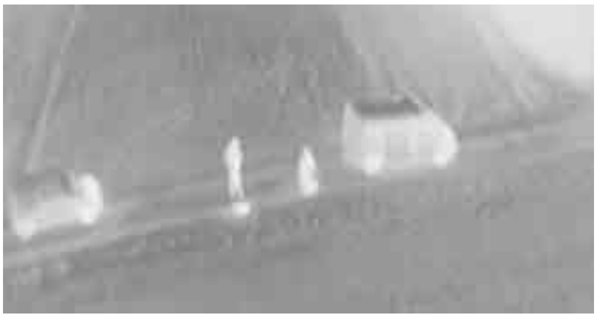

Fig. 6. A surveillance image shot from a highly equipped micro uav drone.

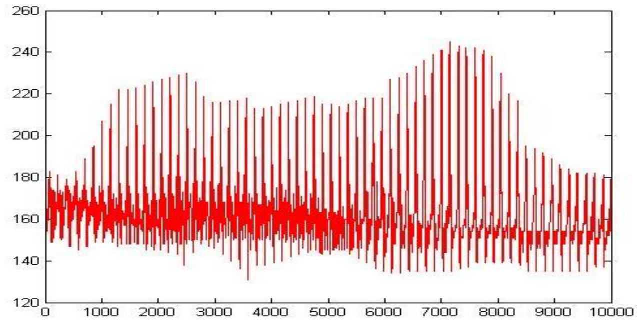

Fig. 7. A graph of the first 10000 pixel value of the plain image in figure 6

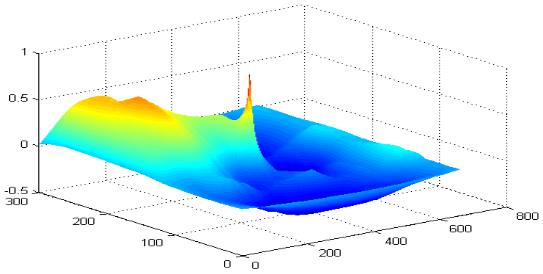

Fig. 8. The graph of the normalized cross-correlation of the matrices of the plain image in figure 6

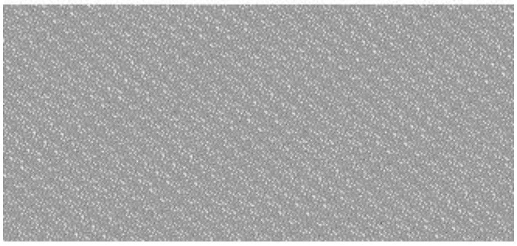

Fig. 9. The resulted ciphered image of the plain image in figure 6

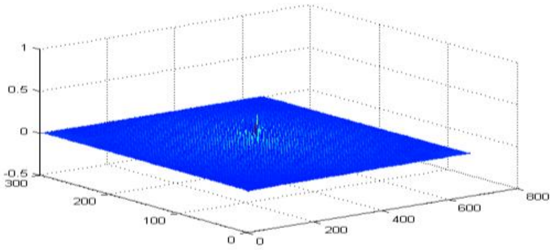

Fig. 10. A graph of the normalized cross-correlation of the matrices of the ciphered image in figure 9

.

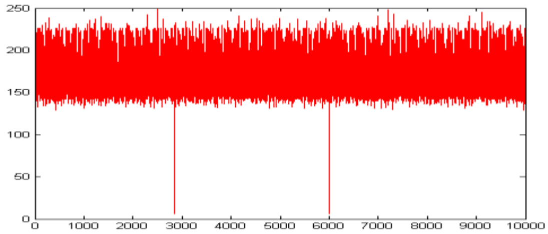

Fig. 11. A graph of the first 10000 pixel value of the ciphered image in figure 9

The plain image in figure 6 above is the mxn image used for the analysis with its first 10000 pixel values plotted above. The entropy of the RGB pixel values was found to be 5.7909, 5.7878, and 5.7878. The overall image has entropy to be 5.788833333. The arithmetic mean of the RGB pixel values of the plain and the ciphered image was found to be 163.330, 163.3744, and 163.3744. The overall image has entropy to be 163.3596333.

5. CONCLUSIONS

The hybrid nature of the procedure engaged in this work involving key-exchange algorithm makes it easy for encryption process to be done involving two or more parties or nodes which provided authentication, confidentiality and integrity to the cryptographic method. The non pixel loss aspect after the encryption process makes it suitable for the encryption and securing of images that needs to preserve information.

Our Future works will involve post quantum cryptographic approaches and hybrid forms of the implemented technique by engaging pixel values and keys.

6. ACKNOWLEDGMENT

This work was supported by Lab-STICC (UMR CNRS 6285) at UBO France, AWBC Canada, Ambassade de France-Institut Français-Ghana and the DCSIT-UCC, and also Dominique Sotteau (formerly directeur de recherche, Centre national de la recherche scientifique (CNRS) in France and head of international relations, Institut national de recherche en informatique et automatique, INRIA) and currently the Scientific counselor of AWBC.

7. REFERENCES

[1] Balfour, R.E.; Donnelly, B.P., "The what, why and how of achieving urban telepresence," Systems, Applications and Technology Conference (LISAT), 2013 IEEE Long Island , vol., no., pp.1,6, 3-3 May 2013doi: 10.1109/LISAT.2013.6578234

[2] Yun-Ju Huang, Feng-Hao Liu, and Bo-Yin Yang. 2012. Public-Key cryptography from new multivariate quadratic assumptions. In Proceedings of the 15th international conference on Practice and Theory in Public Key Cryptography (PKC'12), Marc Fischlin, Johannes Buchmann, and Mark Manulis (Eds.). Springer-Verlag, Berlin, Heidelberg, 190-205. DOI=10.1007/978-3-642-30057-8_12 http://dx.doi.org/10.1007/978-3-642-30057-8_12

[3] Benny, Applebaum, Boaz Barak, and Avi Wigderson. 2010. Public-key cryptography from different assumptions. In Proceedings of the forty-second ACM symposium on Theory of computing (STOC '10). ACM, New York, NY, USA, 171-180. DOI=10.1145/1806689.1806715 http://doi.acm.org/10.1145/1806689.1806715

[4] Ray, A. Perlner and David A. Cooper. 2009. Quantum resistant public key cryptography: a survey. In Proceedings of the 8th Symposium on Identity and Trust on the Internet (IDtrust '09), Kent Seamons, Neal McBurnett, and Tim Polk (Eds.). ACM, New York, NY, USA, 85-93. DOI=10.1145/1527017.1527028 http://doi.acm.org/10.1145/1527017.1527028

[5] Musheer Ahmad and Tanvir Ahmad. 2014. Securing multimedia colour imagery using multiple high dimensional chaos-based hybrid keys. Int. J. Commun. Netw. Distrib. Syst. 12, 1 (November 2014), 113-128. DOI=10.1504/IJCNDS.2014.057991http://dx.doi.org/ 10.15 04/I J CNDS.2014.057991

[6] Jonathan Bishop. 2014. Representations of 'trolls' in mass media communication: a review of media-texts and moral panics relating to 'internet trolling'. Int. J. Web Based Communities 10, 1 (December 2014), 7-24. DOI=10.1504/IJWBC.2014.058384 http://dx.doi.org/ 10.1504/IJWBC.2014.058384

[7] Sajal, K. Das, Krishna Kant, and Nan Zhang. 2012. Handbook on Securing Cyber-Physical Critical Infrastructure (1st ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[8] Bjorkbom, M.; Timonen, J.; Yigitler, H.; Kaltiokallio, O.; Garcia, J.M.V.; Myrsky, M.; Saarinen, J.; Korkalainen, M.; Cuhac, C.; Jantti, R.; Virrankoski, R.; Vankka, J.; Koivo, H.N., "Localization Services for Online Common Operational Picture and Situation Awareness," Access, IEEE , vol.1, no., pp.742,757, 2013 doi:10.1109/ACCESS.2013.2287302

[9] Saeed, Q.; Basir, T.; Ul Haq, S.; Zia, N.; Paracha, M.A., "Mathematical Hard Problems in Modern Public-Key Cryptosystem," Emerging Technologies, 2006. ICET '06. International Conference on , vol., no., pp.456,460, 13-14 Nov. 2006 doi: 10.1109/ICET.2006 .335986

[10] He, Jun; Jun Zheng; Zhi-bin Li; Hai-feng Qian, "Color Image Cryptography Using Multiple One-Dimensional Chaotic Maps and OCML," Information Engineering and Electronic Commerce, 2009. IEEC '09. International Symposium on , vol., no., pp.85,89, 16-17 May 2009 doi: 10.1109/IEEC.2009.23

[11] Ming, Sun Fu; Au, O.C., "Joint visual cryptography and watermarking," Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on , vol.2, no., pp.975,978 Vol.2, 30-30 June 2004 doi: 10.1109/ICME.2004.1394365

[12] ShunDa Lin, "Image transmission and cryptography on the basis of Mobius transform," Image and Signal Processing (CISP), 2012 5th International Congress on , vol., no., pp.258,261, 16-18 Oct. 2012 doi: 10.1109/CISP.2012.6469901

[13] Singh, T.R.; Singh, K.M.; Roy, S., "Robust video watermarking scheme based on visual cryptography," Information and Communication Technologies (WICT), 2012 World Congress on , vol., no., pp.872,877, Oct. 30 2012-Nov. 2 2012 doi: 10.1109/WICT.2012.6409198

[14] Kester, Q. A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., & Quaynnor, N. N. (2014). A hybrid encryption technique for securing biometric image data based on feistel network and RGB pixel displacement. In Recent Trends in Computer Networks and Distributed Systems Security (pp. 530-539). Springer Berlin Heidelberg.

[15] Dongming, Chen, "A Feasible Chaotic Encryption Scheme for Image," Chaos-Fractals Theories and Applications, 2009. IWCFTA '09. International Workshop on , vol., no., pp.172,176, 6-8 Nov. 2009 doi: 10.1109/IWCFTA.2009.43

[16] Prema, G.; Natarajan, S., "An enhanced security algorithm for wireless application using RSA and genetic approach," Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on , vol., no., pp.1,5, 4-6 July 2013 doi: 10.1109/ICCCNT.2013.6726679

[17] Bansod, S.P.; Mane, V.M.; Ragha, L.R., "Modified BPCS steganography using Hybrid cryptography for improving data embedding capacity," Communication, Information & Computing Technology (ICCICT), 2012 International Conference on , vol., no., pp.1,6, 19-20 Oct. 2012 doi: 10.1109/ICCICT.2012.6398199

[18] Kester, Q. A., & Koumadi, K. M. (2012, October). Cryptographie technique for image encryption based on the RGB pixel displacement. In Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on (pp. 74-77). IEEE.

[19] Bruen, Aiden A. & Forcinito, Mario A. (2011). Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. John Wiley & Sons. p. 21. ISBN 978-1-118-03138-4. http://books.google.com/books?id=fd2LtVgFzoMC& pg=PA21.

[20] R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21 (2), pp.120-126. 1978.

[21] SQUAD X CORE TECHNOLOGIES SEEKS TO BRING TECHNOLOGICAL ADVANCES TO THE INFANTRY(2015) New program pursues integrated systems to enhance infantry squad adaptability and flexibility in complex environments SQUAD http://www.darpa.mil/NewsEvents/Releases/2015/02/09a .aspx

[22] Disarmament and International Security Committee.(2014) The Use of Drones and Autonomous Robots. Bucharest international model united nation congress.