A Cryptographic and Watermarking Encryption Technique for Securing and Authentication of Digital Images

Quist-Aphetsi Kester[123], 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
Identity management is crucial in cyberspace where infringement of one's privacy, copy right disputes, theft and other malicious activities are very rampant. There exists a need of ownership identification and authentication of digital images. In solving and contributing to this field, we proposed a cryptographic and watermarking encryption technique for securing and authentication of digital images for identity management. In our approach, we encrypt the data to be embedded into the image before embedding it to the image. We make sure we select a random position in the image based on an embedding key. We make sure the message to be embedded was converted into values that falls in between 0-255. This is to avoid it being detected using forensic or steganalytic software.

General Terms
Security, Cryptography, watermarking, image processing

Keywords
Digital image, encryption, authentication, watermarking

1. INTRODUCTION
Identity management, proof of ownership, etc are very vital approaches used in digital images. Security of digital images in today's cyberspace is very crucial due to the automation of business processes and all other activities that have a major impact on the way transactions are carried out daily. Digital images, videos and other formats of multimedia find its way onto websites ranging from entertainment, to government, education etc. Intellectual property of creativities in digital formats can easily be duplicated and used in other forms without the permission or authorization of the rightful author of such property and these puts the owner at a disadvantaged position. A proof of ownership of such files becomes very difficult for digital forensics expert to work on if there exists to trace that can be used to reach the rightful owner or the original creator. Contrary to the forensic tools too, there are a lot of off the shelf forensic tools are image analysis tools that can be used to detect watermarks or embedded information into such images to make them disguisable. Watermarks within images can be seen if they can visually be seen in the image. Such visible watermarks can easily be detected and altered or replaced with another one. This makes visible watermarks vulnerable to attacks. Some watermarks also have a transparent application approaches or are invisible or blind to the naked eye. Blind watermarks which are also embedded into images cannot be seen but can be detected using tools and techniques. Even though blind watermarks are effective, they are exposed a lot of possible attacks based on the use of some off the shelf software. Some people hybrid approaches by engaging steganographic software or approaches in embedding the message. But once the message is detected, the approach becomes vulnerable to attacks. Steganographic approaches can easily be detected using steganalytic software. The embedding capacity of such images too can be very limited due to the space available. In the avoidance of all these we introduced our approach in which we make data to be embedded part of the pixel values and data type of the image making it very difficult to detect without the knowledge of the original image. By employing cryptographic approach in the process, we make the data embedded disguisable to be obtained in raw and understood. We built an application for the implementation and perform analysis on the results. The paper has the following structure: section 2 related works, section 3 Methodology, section 5 results and analysis, and section 6 concluded the paper.

2. RELATED WORKS
Aslantas, et al in their paper of "A new SVD based fragile image watermarking by using genetic algorithm." proposed a novel fragile image watermarking scheme based on singular value decomposition (SVD) using genetic algorithm (GA) by using multiple scaling factors (SFs). The image was divided into blocks and the watermarked image was obtained by embedding a different line of the watermark to singular values (SVs) of the every block. When an attack does not occur, exactly the original extracted watermark is obtained; on the other hand, the extracted watermark is intensely distorted [1]. Hu, W. C. et al in their work of "Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes", proposed an effective image forgery detection scheme that identifies a tampered foreground or background image using image watermarking and alpha mattes. The component-hue-difference-based spectral matting was used to obtain the foreground and background images based on the obtained alpha matte. Next, image watermarking based on the discrete wavelet transform, discrete cosine transform, and singular value decomposition was used to embed two different watermarks into the foreground and background images, respectively. Finally, the difference between the obtained singular values was used to detect tampering of foreground or background image [2]. Liu, S., et al in their work of "Robustness of Double Random Phase Encoding spread-space

spread-spectrum watermarking technique" proposed image watermarking scheme, in which the watermark was chosen to be in the form of a digital barcode image, was numerically encrypted using a simulation of the optical DRPE process. This process yielded a random complex image, which was then processed to form a real valued random image with a low number of quantization levels. This signal was added to the host image. Extraction of the barcode, involves applying an inverse DRPE process to the watermarked image followed by low pass filtering. This algorithm was designed to utilize the capability of the DRPE to reversibly spread the energy of the watermarking information in both the space and spatial frequency domains. The uniqueness of the watermark was demonstrated, and it was shown that the DRPE SS-SS has very low false positive errors, and that the larger the barcode width, the lower the false positive rate [3]. Ali, M., et al in their work of "An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony" proposed a blind color image watermarking scheme based on quaternion discrete Fourier transform (QDFT) and on an improved uniform log-polar mapping (IULPM). The watermarking scheme embeds dual watermarks: one was a meaningful binary image watermark and the other is a bipolar watermark. The former was embedded in the real part of mid-frequency QDFT coefficients using quantization index modulation. The latter was used to resynchronize the watermark after the watermarked image has been attacked, making the scheme resistant to geometric attacks. Their experimental results demonstrated that the proposed scheme achieved better performance of robustness against both common signal operations and geometric attacks compared to other existing schemes [4]. Chowdhury, et al in their work of "A New DWT-SVD Based Image Watermarking Technique by Utilizing the Features of Human Visual System" proposed an image watermarking methodology that was robust against attacks as well as transparent to human eye. In their work, the horizontal subband of first level DWT of host image was used for higher level decomposition. The singular values of second level horizontal coefficients were modified instead of modifying the DWT coefficients directly by the watermark imag [5]. 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 [6]. Cryptography as an important technique to keep private data secretly in order to avoid unauthorized access makes use of traditional encryption methods such as DES, RSA etc... Chaotic encryption of an image encryption scheme in which shifting the positions and changing the grey values of image pixels are combined simultaneously to ensure a high level of security was proposed by Dongming Chen. Arnold cat map was used to permute the positions of the image pixels in the spatial domain [7].The engagement of hybrid approaches in cryptography has proven to be a more convenient approach in securing data communications. [8] 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 [9]. There exist other forms of approaches such as [10-15].

3. METHODOLOGY

In our approach, we obtain a plain image PI, and a message M with a shared secret key K. The message is converted from other formats to numeric al values where they fall between 0-255 and then transposed and aligned into one dimensional format with a three digit positions per character. The encrypted message was then embed into the image using secret shared key which determines the random chosen positions to embed the message. The entire process is described in the figure below.

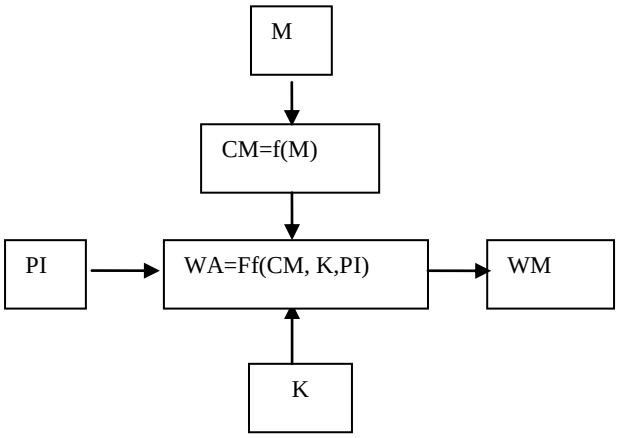

Fig. 1. The summary of the process engaged

From the above image:
PI=Plain Image
K=chosen shared key
M=Watermark data
WA=Watermarking approach
WM=Watermarked Image

We assume the following definition for our approach:

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

Let the watermark data be M to be embedded in PI,

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

Let the shared key K, be

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

Let the channels of PI be R, G, B ∈ PI
$(R \text{ o } G)_{ij} = (R)_{ij}.(G)_{ij}$ and x ∈ [i, j ,m,n] and {x ∈ I: 1 ≤ x ≤+∞}
For x ∈ [R, G, B]: [a, b] = {x ∈ I: a ≤ x ≥ b} where a=0 and b=255

R= r= PI (m, n, 1) **(4)**
G= g= PI (m, n, 1)
B=b= PI (m, n, 1)

M will be in the form of M={x1, x2, x3,…….xn} **(3)**

The following steps were used in the embedding process:

a) Initialize the random number generator to select positions to store the message based on the key, K.
b) Translate a password into an offset value.
c) Process the message, M, for embedding.
d) Pick a random pixel and RGB component based on the key.
e) Get the pixel's color components.
f) Get the value we must store.
g) Update the color.
h) Set the pixel's color.

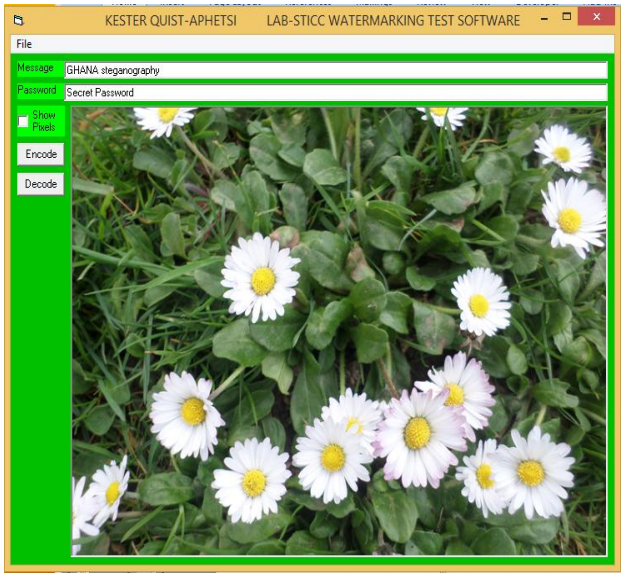

Fig. 2. The developed application for the process using visual basic

An application was developed based on the proposed approach and the generated results were analyzed and shown below in the section that followed.

4. RESULTS AND ANALYSIS

The plain image engaged has a dimension of 640x480 which implies a width of 640 pixels and height of 480 pixels with a bit depth of 24 and a size of 9216454 bytes. The ciphered key engaged is shown in table 1 below.

Fig. 3. The plain image engaged.

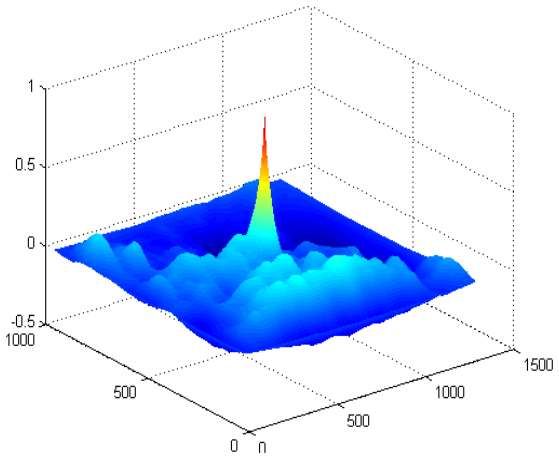

Fig. 4. The graph of the normalized cross-correlation of the matrices of the plain image

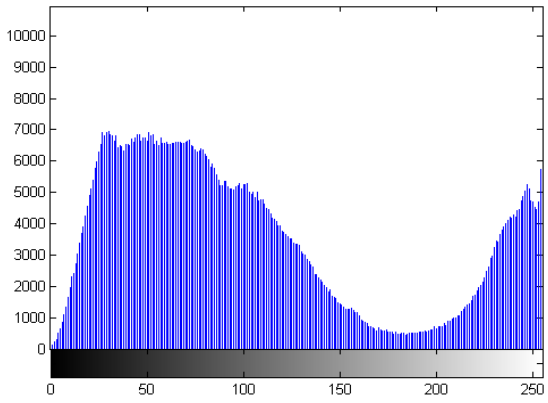

Fig. 5. Histogram of the plain image

Table 1. Table of ciphered key engaged

053	226	169	248	157	071
149	113	063	074	053	037
073	215	158	040	063	164
045	150	072	010	093	061
121	006	064	057	019	090
178	123	011	165	112	002
118	028	125	052	090	040
067	010	091	089	217	074
075	175	146	224	203	093
068	134	109	074	043	207
041	038	090	114	131	188
091	225	140	047	027	138
224	064	022	114	193	018
088	094	238	042	188	112

The data embedded is 252 bytes. After embedding it into the image, the results are shown below:

Fig. 6. The watermarked image

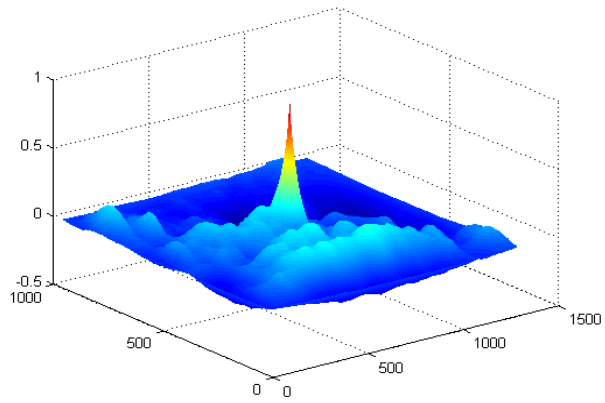

Fig. 7. A graph of the normalized cross-correlation of the matrices of the watermarked image

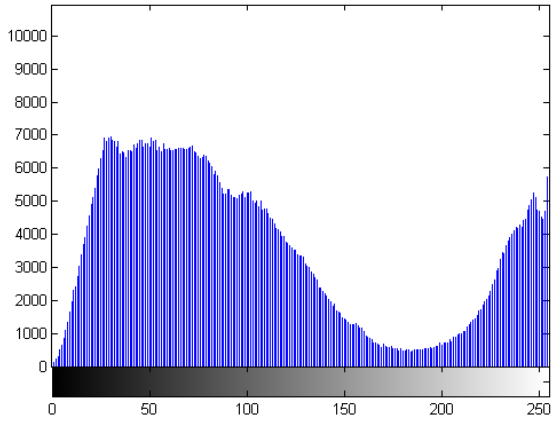

Fig. 8. Histogram of the watermarked image

The plain image and the watermarked images have an entropy value of the RGB pixel values as 7.634492614362974 and 7.634544396435683 respectively. The overall image has entropy to be 5.788833333. The arithmetic mean of the RGB pixel values of the plain and the watermarked image were found to be 106.0928656684028 and 106.0925944010417 respectively.

5. CONCLUSIONS

The results proved to be very effective and the defect in the watermarked image compared with the plain image is very difficult to detect and cannot be visually distinguished. This can clearly be seen in the results of the entropy value of the RGB pixel values as 7.634492614362974 and 7.634544396435683 respectively and its approximation to four decimal places will reflect no change in image. This makes it more difficult to track change. And since the values embedded become part of the pixel values of the image, steganalytic software will yield no results in the process of its analysis. Hence the watermarking remained blind to third parties.

Our future work will be focused on hybrid approaches with other forms of embedding techniques in different domains engaging different methods.

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] Aslantas, Veysel, and Mevlut Dogru. "A new SVD based fragile image watermarking by using genetic algorithm." Sixth International Conference on Graphic and Image Processing (ICGIP 2014). International Society for Optics and Photonics, 2015.

[2] Hu, W. C., Chen, W. H., Huang, D. Y., & Yang, C. Y. (2015). Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes. Multimedia Tools and Applications, 1-22.

[3] Liu, S., Hennelly, B. M., Guo, C., & Sheridan, J. T. (2015). Robustness of Double Random Phase Encoding spread-space spread-spectrum watermarking technique. Signal Processing, 109, 345-361.

[4] Ali, M., Ahn, C. W., Pant, M., & Siarry, P. (2015). An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. Information Sciences.

[5] Chowdhury, A., Shahjamal, M., & Biswas, K. (2015). A New DWT-SVD Based Image Watermarking Technique By Utilizing The Features Of Human Visual System. International Journal of Research in Computer Engineering & Electronics, 3(6).

[6] Kester, Quist-Aphetsi, Laurent Nana, Anca Christine Pascu, Sophie Gire, Jojo Moses Eghan, and Nii Narku Quaynnor. "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, 2014.

[7] 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

[8] 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

[9] 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

[10] Quist-Aphetsi Kester,"Image Encryption based on the RGB PIXEL Transposition and Shuffling",IJCNIS, vol.5, no.7, pp.43-50,2013. DOI: 10.5815/ijcnis.2013.07.05

[11] Qian, Z., Zhang, X., & Ren, Y. (2015). JPEG encryption for image rescaling in the encrypted domain. Journal of Visual Communication and Image Representation, 26, 9-13.

[12] Som, S., Sen, S., Mahapatra, S., & Palit, S. (2015). A Selective Bitplane Based Encryption of Grayscale Images with Tamper Detection, Localization and Recovery Based on Watermark. In Information Systems Design and Intelligent Applications (pp. 793-802). Springer India.

[13] Jiang, D., & Kim, J. (2015). A Spread Spectrum Zero Video Watermarking Scheme based on Dual Transform Domains and Log-Polar Transformation. International Journal of Multimedia & Ubiquitous Engineering, 10(4).

[14] Zhang, X., Wang, J., Wang, Z., & Cheng, H. (2015). Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography.

[15] Irene, J., Prabu, U., Gomathi, V., Tejaswini, M. K., Kavipriya, M., & Kumar, K. P. (2015, March). Random Grid and Deterministic Visual Cryptography with Enhanced color patterns. In Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015) (p. 65). ACM.

.