A Spatial Domain Watermarking Approach for Digital Images based on Image Features built on Formal Concepts Analysis

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
A proof of ownership based on digital forensics evidence is the way forward in solving ownership disputes in the ever growing cyberspace that confronts us today. A strong proof beyond all reasonable doubts with the good standing of the law provides victory for a case before a competent court of law. The Society we live in is governed by laws and laws need evidence to pass judgments and not any kind of evidence but evidence compelling enough to attract the passing of judgment. Lessons learnt from the past of the failures of the court to provide and use strong verified evidence due to limitations of scientific evidence such as DNA, surveillance videos, authenticable images etc. have cost human life's freedom and having access to a fair trial. We cannot wait till certain loopholes are exploited in our digital cyber evolution before we get it fixed. Hence stronger and a more compelling techniques are needed for image authentication and identification. In our work, we proposed a spatial domain watermarking approach for digital images based on image features built on formal concepts analysis. We adopt the use of formal concept analysis due to the fact that a change in a pixel value can result in a change in the lattice generated from the image. We presented our results and they showed to be very effective.

General Terms
Security, watermarking, image processing

Keywords
Formal Concept Analysis, Digital image, encryption, authentication, watermarking

1. INTRODUCTION
A world with high dependency on digital information processing cannot do without digital evidence in solving cases. The cyber world has interconnected with the physical world over the decades in such a way that the cyber –physical relationships will be hard to do away with. Collection of multimedia data through surveillance devices are of key interest to the law enforcement agencies as well private property and home owners. Evidence collected by these devices in one way or the other are used to support actions being taken by then in a form of defense or a support to prosecute an individual. Hence these collected data needs various levels of authentication and security. Police are are now encouraged to wear body cameras inline of their duty besides their dash camera on their patrol vehicles in other to collect a vital and supporting evidence for to justify a course of an action. State buildings and public places now have cameras including those that have biometric data collection capabilities in screening and observing events at public places. These devices record crime and they are presented to the law courts as compelling evidences in support of a case before them. Private businesses and home owners adopt such way of collecting evidence to using an eye witness. The digital images present stronger evidence to an eye witness's narration and the evidences derived from these digital devices can be compelling enough for the prosecution of a person.

So reliable as a court of competent jurisdiction may be on these evidences as a compelling proof of passing effective prosecution may be dangerous to the fair trial of a person under prosecution if the footage obtained or the images do not have a forensically authentic support. Yet still as cyber security experts, we are fully aware that the strength of our dependence on digital evidence depends on the time of the technology deployed as well as the availability of the knowledge of potential alterations capable by an adversary in messing up with the evidence or altering it. No matter how strong a forensic process may be in a case today, its relevance in tomorrow's case by referencing may be useless. This is because case laws are the bedrock of most law courts rulings and referral to the engagement of techniques as well.

Therefore the need for a one step ahead forensics technique is of a key importance when considering forensics approaches. Henceforth evolving techniques of digital evidence have to be deployed in the verification and authentication of collected or stored digital multimedia data. Forensic data may be stored in the cloud. These cloud storage locations can be private or public. Cloud security is mainly limited to access security and only few provide data security with user level authentication. This is because firms also have to mine cloud data for other unauthorized purposes like for marketing etc. But Forensic data are now finding their ways into the cloud in order to support distributed nature of policing activities as well as easy access to interconnected crime labs or databases. Authentication in change or validity of these digital images is very crucial for criminal proceedings hence we proposed an approach in contribution to the solutions that exists in these domains. Our approach has to work in spatial domain on the pixel values due to the dependency of the composed image on the data. A change in the image can easily be detected by our proposed approach. The following sections explains our adopted approach. 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

Identity management, authentication, confidentiality and integrity of transmitted multimedia have evolved ever since the beginning of the commercialization and globalization of the interconnection of communication networks. Som, S., Palitet al in their work of "A DWT-based Digital Watermarking Scheme for Image Tamper Detection, Localization, and Restoration" proposed a discrete wavelet transform (DWT)-based watermarking scheme for image tamper detection, localization and restoration. In their scheme, the original image was first partitioned into blocks of size 2 × 2 in which a 1D DWT was applied to produce the watermark which was embedded in four disjoint partitions of the image to enhance the chance of restoration of the image from different cropping attack-based tampers. The validity and superiority of the proposed scheme was verified through extensive simulations using different images of two extensively used image databases [1]. Shao, Z., et al in their work of "Combining double random phase encoding for color image watermarking in quaternion gyrator domain" proposed a scheme of an RGB-scale watermark image together with a grayscale watermark image or not is encoded into a quaternion matrix and encrypted through the DRPE, the encrypted data is then fused into the middle coefficients of the quaternion gyrator-transformed host image. In the process of extracting watermarks, it is impossible to retrieve them without authorized keys. Compared with the three channels independently processing approach implemented in fractional Fourier domain, the proposed algorithm achieves lower complexity by reason of avoiding repetitive operations. Experimental results have demonstrated the feasibility of the proposed algorithm and its superior performance in terms of noise robustness [2]. Hyung-Kyo Lee et al intheir work of "ROI Medical Image Watermarking Using DWT and Bit-plane," proposed digital watermarking technique for medical image that prevents illegal forgery that can be caused after transmitting medical image data remotely. This approach was adopted to avoid wrong diagnosis likely to occur if the wrong image is used. In their approach, they embed the watermark into some area of medical image, except the decision area that made a diagnosis so called region of interest (ROI) area in their work, to increase invisibility. The watermark is the value of bit-plane in wavelet transform of the ROI for integrity verification. The experimental results show that the watermark embedded by the proposed algorithm can survive successfully in image processing operations such as JPEG lossy compression [3]. Na Liet al in their work of "Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform," proposed a technique for digital image watermarking based on DWT. Their technique worked by adding binary image watermark to gray image and the host image. Their approach adopted two characteristics: for the first part was adaptation of various gray images and the second part engages Arnold transform pretreatment to remove spatial correlation and disperses the error bits among all pixels to make watermarking more strongly robust against cropping operation. At the end, their outputs indicated that the proposed technique was invisible and robust against common image processing and cropping operation [4]. In their work, Arnold transform was applied to binary image, that was watermarking pretreatment, and randomized image was embedded as watermarking to produce watermarking image. The Arnold transform that was applied to every pixel in the image is given by the formula in matrix notation:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod } N) \quad (1)$$

x,y).{0,1,…,N-1}are the pixel coordinates from original image and (x′,y′)are corresponding results after Arnold transform

$$F'(u,v) = F\ (u,v)(1 + \delta^{*}\, w(u,v)) \quad (2)$$

Jiang Xuehua in their work of "Digital Watermarking and its Application in Image Copyright Protection", proposed a system model of a digital watermarking. The system consisted of two modules which were watermark embedding module and watermark detection and extraction module. In view of the importance of digital images copyright protection, based on the analysis of the main digital watermarking algorithms, the digital watermarking technology could be applied to the image copyright protection. The two dimension discrete cosine transform wad encoded on the Windows platform by using Visual C++ program language. The experiment result showed that the digital watermark was non-perceptible, the watermark information can be extracted even if it had been attacked, and the expected effect can be achieved [5]. Below is the description of the process.

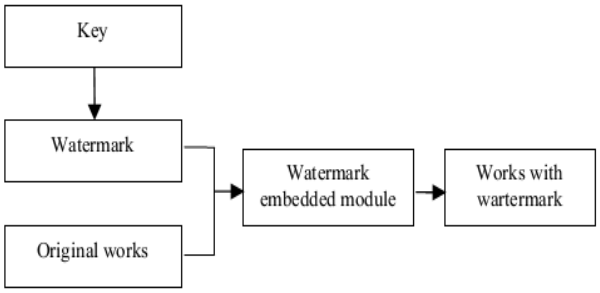

Fig. 1. The description of the process engaged in [5]

Rawat, N., Kim et al in their work of "Compressive sensing based robust multispectral double-image encryption" showed a multispectral double-image-based encryption system that took advantage of only a tiny number of random white noise samples for a decryption process. Mathematical and numerical simulations were carried out on the process to verify the feasibility as well as the robustness of their proposed system and results were presented in order to demonstrate the effectiveness of the proposed system [6]. Liu, H., Kadir, Aet al in their work of "A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise", engaged a three S-Boxes that was generated by a complex chaotic system and each of the S-box randomly generated was engaged in turns to encrypt one of the color components in each pixel adhering to the switching sequence, which is also generated by the complex chaotic system. Their results showed the effectiveness of the scheme as suitable for color image encryption [7].

Formal Concept Analysis (FCA) is is a field of applied mathematics based on the mathematization of concept and conceptual hierarchy. It thereby activates mathematical thinking for conceptual data analysis and knowledge processing [8]. Formal Concept Analysis has been originally developed as a subfield of Applied Mathematics based on the mathematization of concept and concept hierarchy. Only after more than a decade of development, the connections to the philosophical logic of human thought became clearer and even later the connections to Piaget's cognitive structuralism which Thomas Bernhard Seiler convincingly elaborated to a comprehensive theory of concepts in his recent book [9].

Formal Concept Analysis has typically been applied in the field of software engineering to support software maintenance and object-oriented class identification tasks. This paper presents a broader overview by describing and classifying academic papers that report the application of FCA to software engineering. The papers are classified using a framework based on the activities defined in the ISO12207 Software Engineering standard [10]. Due to the uniqueness of generated lattices in maintaining their concepts unless disturbed, we based our unique watermarking features extracted from the lattice in a manner that a change in the lattice will result in a change in the extracted features and we also used the lattice in our image authentication.

3. METHODOLOGY

In our approach, we extract the frequency of occurrence of each element from the image and construct the lattices based on the arithmetic mean, standard deviation, and entropy values extracted from the image. We use the data from the lattice as well as from the plain image as our watermarking data. This approach makes the watermark unique for each image that will be engaged in this process. A change in the image will result in the lattice but the change of the lattice will only affects the affected concepts of the image, this produces a good level of the extracted data against attacks. Below is the figure 2 showing the summary of the process engaged :

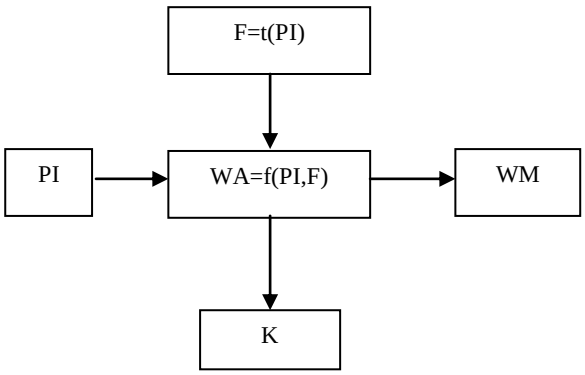

Fig. 2. The summary of the process engaged

From the above image:
PI=Plain Image
F=Feature extraction
M=Watermark data
WA=Watermarking approach
WM=Watermarked Image

We assume the following definition for our approach:

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

Let X=freq(x) frequency in r,g and b

$$f = \sum_{i=m}^{n} X_i \quad (4)$$

$$a = \frac{\sum_{i=m}^{n} X_i}{k} \quad (5)$$

Where x ∈ b_i1 : [a, b]= {x ∈ I: a ≤ x ≥ b}

$$s = \sqrt{\frac{1}{N}\sum_{i=m}^{n}(xi - u)^2} \quad , where \;\; u = \frac{1}{N}\sum_{i=m}^{n} x_i \quad (6)$$

Entropy = e

$$e = -\sum \eta = 0\, \varepsilon - 1\, \Psi(xi).\log 2\,(\Psi(xi)) \quad (7)$$

Where:
δ= Entropy of image
ε = Gray value of an input image (0-255).
Ψ (η) = Probability of the occurrence of symbol η

Formal concept analysis analyzes data which describe relationship between a particular set of objects and a particular set of attributes [11-15]. In FCA a formal context consists of a set of objects, G, a set of attributes, M, and a relation between G and M, I ⊆ G × M. A formal concept is a pair (A, B) where A ⊆ G and B ⊆ M.

If g ∈ A and m ∈ B then (g,m) ∈ I ,or gIm.
A formal context is a triple (G,M,I), where
•G is a set of objects,
• M is a set of attributes
•and I is a relation between G and M.
• (g,m) ∈ I is read as „object g has attribute m.
For A ⊆ G, we define
A´:= {m ∈ M | ∀g ∈ A:(g,m) ∈ I }.
For B ⊆ M, we define dually
B´:= {g ∈ G | ∀m ∈ B:(g,m) ∈I }.
For A, A1, A2 ⊆ G holds:
• A1 ⊆ A2 ⇒ A`2 ⊆A`1
• A 1 ⊆A``
• A`= A```
For B, B1, B2 ⊆ M holds:
• B1 ⊆ B2 ⇒ B_2 ⊆ B_1
• B ⊆ B``
• B`= B```
A formal concept is a pair (A, B) where
• A is a set of objects (the extent of the concept),
• B is a set of attributes (the intent of the concept),
•A`= B and B`= A.

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

$$M = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} & . & . & . & x_{1n} \\ x_{21} & x_{22} & . & . & . & . & . & x_{2n} \\ x_{31} & . & . & . & . & . & . & x_{3n} \\ x_{41} & . & . & . & . & . & . & x_{4n} \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ x_{m1} & .x_{m2} & x_{m3} & x_{m4}. & . & . & . & x_{mn} \end{bmatrix} \quad (8)$$

Let the shared key K, be

$$K = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} & . & . & . & x_{1n} \\ x_{21} & x_{22} & . & . & . & . & . & x_{2n} \\ x_{31} & . & . & . & . & . & . & x_{3n} \\ x_{41} & . & . & . & . & . & . & x_{4n} \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ x_{m1} & . x_{m2} & x_{m3} & x_{m4} . & . & . & . & x_{mn} \end{bmatrix} \quad (9)$$

Let the channels of PI be R, G, B ∈ PI
$(R \circ G)_{ij} = (R)_{ij} . (G)_{ij}$ 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) **(10)**

M will be in the form of M={x1, x2, x3,…….xn} **(11)**

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. 3. 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. 4. The plain image

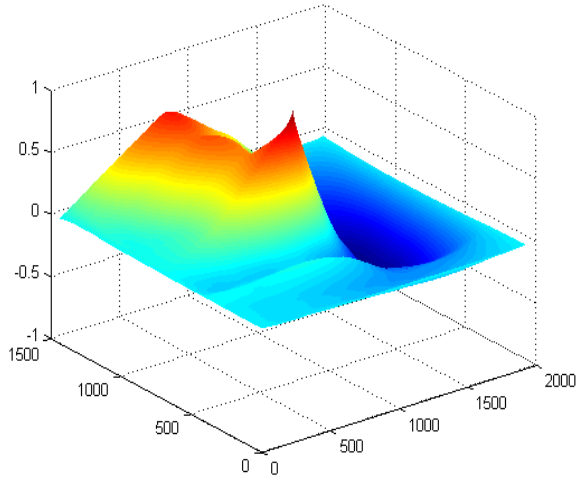

Fig. 5. The graph of the normalized cross-correlation of PI

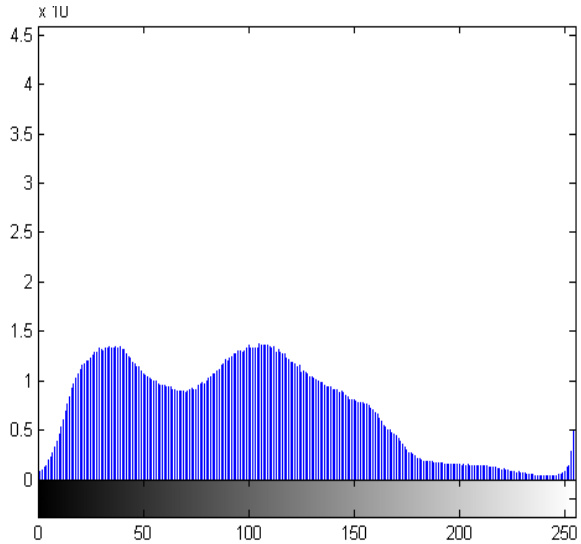

Fig. 6. Histogram of the PI

Table 1: Table Objects X and attributes

G	J	f'	a'	s'
0-25	169938	0.081953	1502.998	2343.901
26-50	316517	0.152641	2799.4	4365.619
51-75	235764	0.113698	2085.189	3251.819
76-100	289149	0.139443	2557.347	3988.141
101-125	319446	0.154054	2825.306	4406.018
126-150	235758	0.113695	2085.136	3251.736
151-175	146001	0.070409	1291.29	2013.746
176-200	46113	0.022238	407.8414	636.0221
201-225	31294	0.015092	276.7764	431.6283
226-255	283620	0.136777	2508.446	3911.881

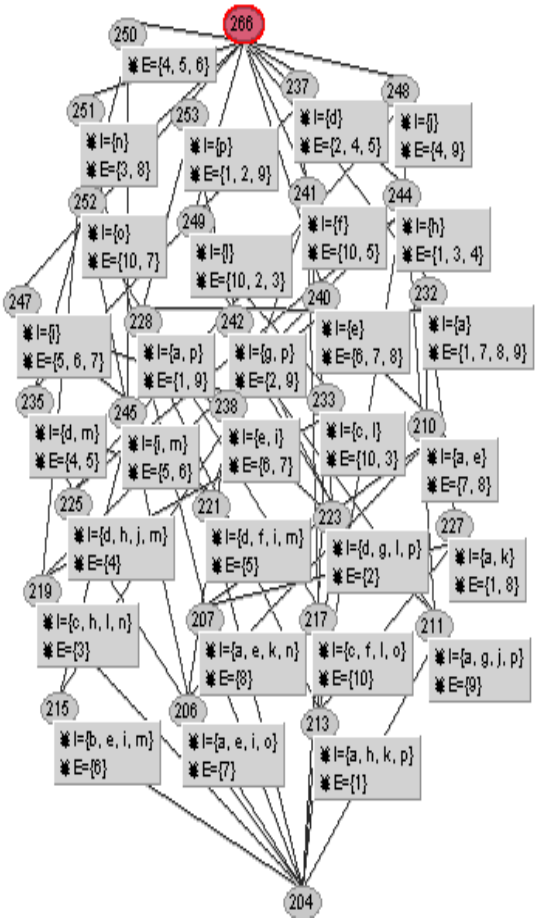

Fig. 7. The lattice from table 1

Fig. 8. The watermarked image WI

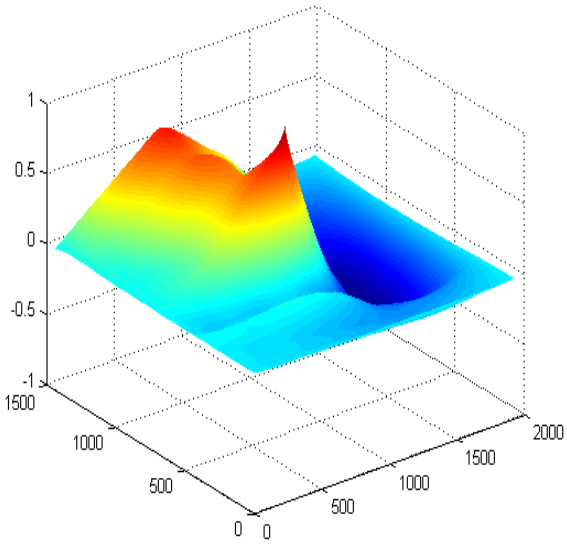

Fig. 9. A graph of the normalized cross-correlation of WI

.

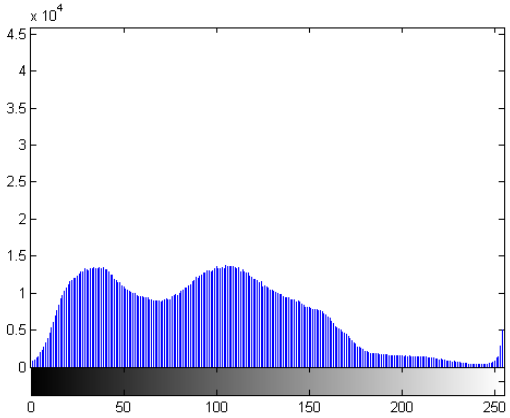

Fig. 8. Histogram of WI

Above is the results from the experiments carried out on the image.

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. Due to the fact that a change in concept will result in a change in lattice makes our approach strongly suitable for analysis and authentication of digital images.

We will engage homomorphic approaches with this technique as well as image indexing and retrieval techniques of ciphered images with encrypted features in our future works.

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] Som, S., Palit, S., Dey, K., Sarkar, D., Sarkar, J., & Sarkar, K. (2015). A DWT-based Digital Watermarking Scheme for Image Tamper Detection, Localization, and Restoration. In Applied Computation and Security Systems (pp. 17-37). Springer India.

[2] . Shao, Z., Duan, Y., Coatrieux, G., Wu, J., Meng, J., & Shu, H. (2015). Combining double random phase encoding for color image watermarking in quaternion gyrator domain. Optics Communications, 343, 56-65.

[3] Hyung-Kyo Lee; Hee-Jung Kim; Seong-Geun Kwon; Jong-Keuk Lee, "ROI Medical Image Watermarking Using DWT and Bit-plane," Communications, 2005 Asia-Pacific Conference on , vol., no., pp.512,515, 5-5 Oct. 2005 doi: 10.1109/APCC.2005.1554112

[4] Na Li; Xiaoshi Zheng; Yanling Zhao; Huimin Wu; Shifeng Li, "Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform," Electronic Commerce and Security, 2008 International Symposium on , vol., no., pp.942,945, 3-5 Aug. 2008 doi: 10.1109/ISECS.2008.140

[5] Jiang Xuehua, "Digital Watermarking and its Application in Image Copyright Protection," Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on , vol.2, no., pp.114,117, 11-12 May 2010 doi: 10.1109/ICICTA.2010.625

[6] Rawat, N., Kim, B., Muniraj, I., Situ, G., & Lee, B. G. (2015). Compressive sensing based robust multispectral double-image encryption. Applied Optics, 54(7), 1782-1793.

[7] Liu, H., Kadir, A., & Gong, P. (2015). A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise. Optics Communications, 338, 340-347.

[8] Ganter, B., & Wille, R. (2012). Formal concept analysis: mathematical foundations. Springer Science & Business Media.

[9] Wille, R. (2005). Formal concept analysis as mathematical theory of concepts and concept hierarchies. In Formal Concept Analysis (pp. 1-33). Springer Berlin Heidelberg.

[10] Tilley, T., Cole, R., Becker, P., & Eklund, P. (2005). A survey of formal concept analysis support for software engineering activities. In Formal concept analysis (pp. 250-271). Springer Berlin Heidelberg.

[11] Chaudron, L., & Maille, N. (2000). Generalized formal concept analysis. In Conceptual Structures: Logical, Linguistic, and Computational Issues (pp. 357-370). Springer Berlin Heidelberg

[12] Bernhard Ganter, Bernhard and Rudolf Wille: Formal Concept Analysis: Mathematical Foundations. Springer, Berlin, ISBN 3-540-62771-5, p. 1

[13] Pascu, A., & Desclés, J. P. (2008). Attribute-Value Formalization in the Framework of the Logic of Determination of Objects (LDO) and Categorization. In FLAIRS Conference (pp. 506-511).

[14] Kester, Q. A., Pascu, A. C., Nana, L, Gire, S., Eghan, J. M., & Quaynnor, N. N. (2015). Feature Based Encryption Technique for Securing Digital Image Data Based on FCA-Image attributes and Visual Cryptography. Lecture Notes in Computer Science. Theoretical Computer Science and General Issues:Computational Science and Its Applications. Springer Berlin Heidelberg.

[15] Kester, Q. A., Pascu, A. C., Nana, L, Gire, S., Eghan, J. M., & Quaynnor, N. N. (2015). Feature Based Encryption Technique for Securing Digital Image Data Based on FCA-Image attributes and Visual Cryptography. In Computational Science and Its Applications–ICCSA 2015. Springer International Publishing.

.