International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Application of Visual Encryption and its Inferences in Data Provenance

Kukatlapalli Pradeep Kumar[1*], Ravindranath C Cherukuri[2]

[1 2] Department of Computer Science and Engineering,
CHRIST (Deemed to be University),
Bangalore, Karnataka, India

[*]*Corresponding Author: kukatlapalli.kumar@christuniversity.in*

DOI: https://doi.org/10.26438/ijcse/v7i5.10881094 | Available online at: www.ijcseonline.org

Accepted: 14/May/2019, Published: 31/May/2019

***Abstract*—** Security is the main aspect of any communications among untrusted networks in the current world. Thanks to many researchers for their enormous contributions on effective security algorithms despite different attacks breaching the weakness on the computer systems. As always, execution of these algorithms used to take time because of their dependency on mathematical analysis. The more the complexity of mathematical model, the more is the robustness of the algorithm though. Good number of them proved to be strong and are used in many popular applications over internet systems for providing security. There were a few of some methods which used very less of the mathematical concepts. One of them and the most widespread schemes is Visual Cryptography. This considers images as one of the important element in its methodology. However, this notion is different from other imagery concepts used in security. The below information gives reader a clear view on visual cryptographic schemes available, and also it provides an understanding on different heterogeneous applications oriented to the same. This paper also focuses on an application oriented aspect of Data Provenance with respect to secure communication.

***Keywords*—** Visual Encryption, Data Provenance, Cyber Security, Attack Investigations

I. INTRODUCTION

Data Provenance is one of the topics which gained a great attention from the researchers in recent days. Information on the web these days is huge. The challenge lies in its correctness and reliability, if it is to be processed for further usage. The origin, birth and path travelled by the data from its inception to the current state are some of the critical and sensitive aspects of data processing. The feature which revolves around the derivation of the history of a specific data is known as Data Provenance. Applications such as intellectual property issues, information processing are tightly coupled with data provenance as an essential part of understanding the ownership of data. There has been many algorithms and different methods proposed, implemented for information security from decades in various application areas.

However, the threats to the data security remains with the technology advancements. All most all of these algorithms and methods, implemented for the data security uses more of complex mathematical calculations. Leaving these complex numerical computations into account, M. Naor and A. Shamir proposed a new theory to encrypt the data efficiently named as 'Visual Cryptography' [36]. This concept is based on stacking the shares available at the individual users, participating in the data transmission for retrieving the original message. Thus, this proposed work emphasizes on providing security for the data with respect to its provenance. The remaining content in this paper take following path. The second section of this paper deals with literature study on visual cryptography on various applications with pictorial illustrations, the third part provides a glimpse on framework for provenance security i.e., visual encryption framework for provenance security. The fourth section deals about the results obtained with the software application. The last section gives the gestalt with conclusion of the paper with respect to a view on proposed problem definition.

II. BACK GROUND AND LITERATURE STUDY ON VISUAL CRYPTOGRAPHY

Various popular and recent research works on visual cryptography were taken into consideration, analysed as a part of literature study. The following section discusses about the same. To deceive the entities accessing the shares in transmitting the sensitive information, shares can be enclosed into evocative images. In order to generate such significant images, watermarking technique is implemented. So the

actual secret image is watermarked with different evocative images and are sent over communication channel. At the other end the cover images are progressively removed from the shares and stacked to know the original image. This has the benefit over the Progressive Visual Cryptography (PVC) scheme [1].

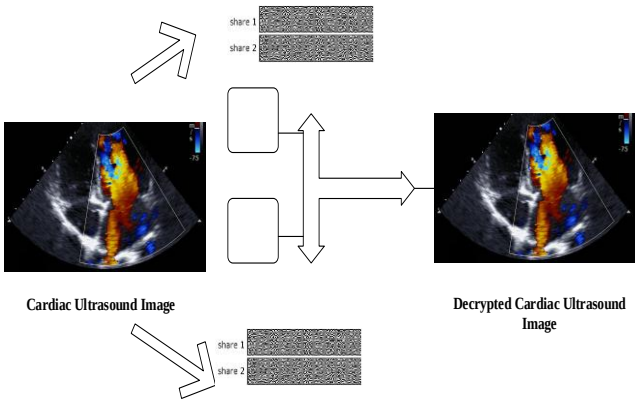

Figure 1. Representation of secret shares with ultrasound images

With the help of a method in visual cryptography, named Visual Secret Sharing (VSS) the medical records such as Electronic Medical Report (EMR), X-ray, CT scan, Ultrasound scan, MRI scan etc., can be securely stored and shared [2]. This is developed with 2-out-of-2 Visual Secret Shares with only black and white pixels which is valid for black and images only. The same method benefits increasing contrast levels of the decrypted image. Figure 1. shows the same.

Visual Secret Sharing (VSS) concept united with CAPTCHA (completely automated public Turing test to tell computers and humans apart) [3, 4] [5] delivers a improved resolution for validating the involved contributors over the untrusted communication networks. This technique also averts the bot attacks finding the flawless difference between human interaction and a bot outbreak. It's the situation of retrieving a system which is permitted with both CAPTCH and VSS. It offers the authorisations for human operator but not to bots or botnets.

The Random Grid (RG) concept focusses visual encryption on pixels without actual expansion. A drawback with afore mentioned approach is, the RG-based visual scheme can be revealed with a rebuilt secret with inferior visual effect as the average light communication of a share is static. In order to overcome the flaw, a generalized RG is proposed with adjustable light transmission of a secret share. This new idea can implement new visual cryptographic (VC) schemes. As an outcome, VC schemes are, the generalized RG and a XOR built expressive VC. The probability of suspicion on secret image encryption is abridged [6]. The region incrementing visual secret sharing (RIVSS) method initially proposed with 2-level incrementing visual cryptography with random grids. The new scheme proposed will have both RIVSS and random grids (RG) combined together to form RGRIVSS [7]. This can deal more than 2-level region incrementing VSS. In-order to enhance the contrast of image in the visual cryptographic scheme (VCS), the XOR operation is used in decoding the shares. A former approach used the OR operation, the OVCS, which tainted the visual feature of recreated image. However, XOR-based VCS, the XVCS [8] contrast was seen improved 2(k-1) times. A new grayscale RCVS (reverse visual cryptography scheme) have been proposed which has less pixel expansion rate to introduce an optimal-contrast grayscale (GRVCS). It used black coloured RCVS in the matrices calculation. This paybacks the diverse requirements from different users/ participants [9]. User friendly visual cryptography scheme (FVCS) [10] is a variation in Visual cryptography. This user friendly shares are generated by extending the probabilistic visual cryptography with entrenched corresponding cover images. This method also helped in adjusting the contrast for the meaningful shares. As the original VCS can easily be tarnished by malevolent participants, the digital watermarking [11] can be applied as an extension to VCS. So the intended recipients can verify validity and authentication of shares by watermark mining operation. Providing security for visual secret sharing (VSS) schemes is a challenge. Iwamoto [12] proposed a weak security notion for VSS. Using this method, the VSS can be secured and can have a robust shield against attackers. Undeniably these are unconditionally secure. The relation between unconditionally secure and weakly secure approaches are studied and a weakly secure VSS was proposed especially for color images. Smaller pixel expansion have been used here in this regard. Improved visual steganography in relation with visual cryptography techniques helps in solving real time issues. This improved technique have been proved to have good performance over other traditional methods especially in banking applications regarding authenticating the internet entities in various transactions [13].

To encode password of customers a method uses nearly eight neighbouring pixels to increase complexity in order to deceive attackers. The encoded frame is divided into 'n' number of shares. If there are 'n' no. of shares drawn from an encoded frame, n/2 are with bank and remaining n/2 with bank customer. The customer has to provide his n/2 shares all through of his transactions with bank. As usual these shares are stacked to get original image. Combination of binary encoding methods and visual encryption schemes helps in securely encrypting the data. Visual encryption schemes does the division of original message in to 'n' number of shares. These shares form a cover data which in turn are formed in to host overt image using specific encoding rules. It comprises four clusters namely identification codes, covert-data dimension codes, sharing matrix dimension codes, and information codes [14]. The test

cases with corresponding test results illustrates that the method has a good performance over traditional methods. The blend of two mechanisms, visual secret sharing and discrete wavelet transform (DWT) yields partitioning of watermark into two binary images termed as shares. The shares are generated as follows. One share is created in the watermark embedding phase, other one is mined from the controversial image when needed. However, for decoding original image both shares have to be available and combined. This proposed scheme [15] reduces the size of the shares and betters from other patterns.

The Figure 2. elucidates about base concept of visual encryption [36] in a pictorial form. The elements in middle of the diagram are the communication entities. Switch, Hubs and communication links are taken into consideration. Visual cryptographic schemes are combined with genetic algorithm approaches and steganographic methods. These indigenous combinations enhances the secured transmissions over the untrusted networks.

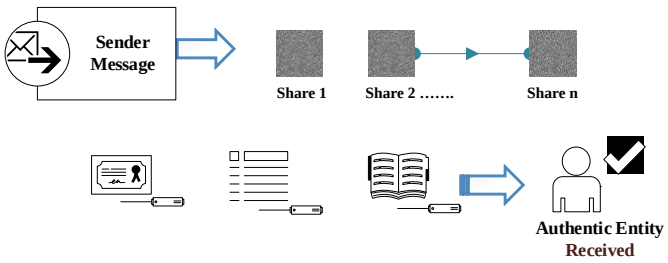

Figure 2. The base concept of visual encryption

In this process original message is altered into a cipher text with a secret key and the same is encapsulated into the least significant bit (LSB) of original image. Genetic algorithm plays a major role in changing the pixel location which makes the detection very difficult. Visual cryptography at this context encrypts the visual information by breaking the image into shares [16]. The performance of the system is verified with steganalysis and benchmarking tests. The extra ability of hiding the confidential data can be obtained by shifting one of the shares for a certain unit in visual cryptography Fang and Lin's scheme [17]. Sometimes it may produce a larger sized image than the original one at recovery. A non-expandable scheme is developed using block encoding with the same added facility of hiding the original data [18].

In order to provide security for shares of the original image in visual cryptography, public key encryption is employed in the data transmission. The RSA algorithm is applied for providing robust security in this regard, it helps in encrypting the secret shares [19]. This method is said to withstand any kind of attacks over internet. The same is shown in Figure 3. The traditional visual cryptographic schemes have issues related to pixel expansion and display quality for the recovered images. To resolve pixel expansion issue a column vector set is designed for encrypting secret pixels. For finest visual cryptographic construction a mathematical model [20] finds the column vectors. Simulated annealing based algorithm is also used in these constructions.

Research work have also been focused on halftone images which has very little size variation between recovered resultant image and original secret image. Pseudo randomization and pixel reversal techniques [21] are used in this process especially for gray scale images information hiding. The visual cryptographic schemes are finding numerous applications in various fields. One of such instances is found in the Internet Voting System (IVS). This has the advantage of voting from a remote area even when there are no election process personnel available. Every one participating in election process is given secure credentials through which they can cast their vote. These credentials follows the visual cryptography methodology. The password is generated by merging the two shares. One share is sent by the administrator at the time of elections to his email address and the other share would be available in voting system. After the user receives the two shares, he/ she has to merge/ stack one on the other to get a password. Through this password as an important credential information, the user can log on to voting system for casting vote. Attacker faces extreme difficulty in this regard to get the shares, as one of them is sent via email [22].

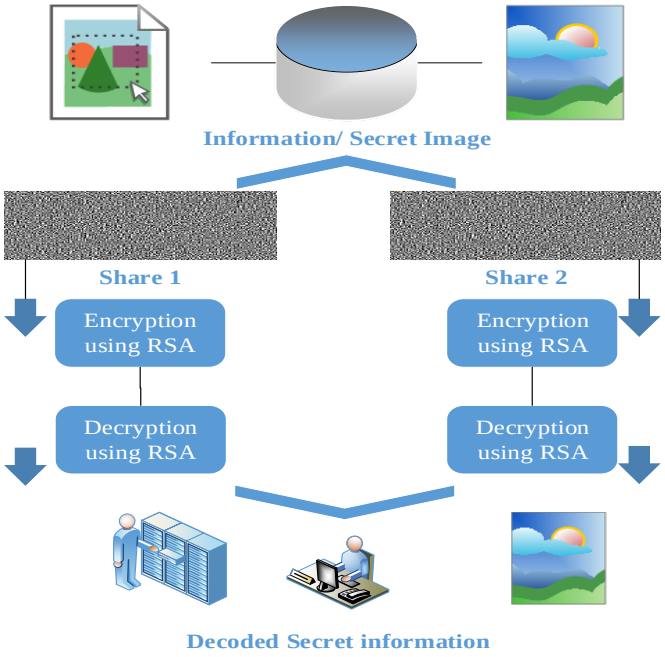

Figure 3: The RSA over Visual Encryption

The traditional visual secret sharing schemes suffer from transmission issues for the secret images/ shares. There is an increase in interception risks observed at the time of transmitting the images for the traditional VSS. To resolve the above mentioned problem, a natural image based visual secret sharing scheme NVSS [23] have been proposed which uses natural images for transmission. This (n, n) – NVSS method can share one digital secret image over n-1 selected natural images, in addition to that a noise-like share can be selected. The noise-like share is produced based on secret image and natural shares. This approach solves the secret image transmission issues to a greater extent. The modified VSS namely NVSS [23] solves the risks in transmission of the secret shares. The proposed approach works for black and white shares, gray-level shares, and color images as well [24] with the same scheme.

Visual cryptographic schemes are used for securing the transmission of videos in military warfare and domestic surveillance especially over drones. Even if the information is attacked and captured, it becomes impossible for the attacker to decipher the same. This is possible by using a new method named quantum key distribution with visual encryption. Key generation is done by quantum key distribution method and this key is used by the encryption technique [25]. Figure 4. pictorially illustrates combination of both techniques for securing video images in military drones.

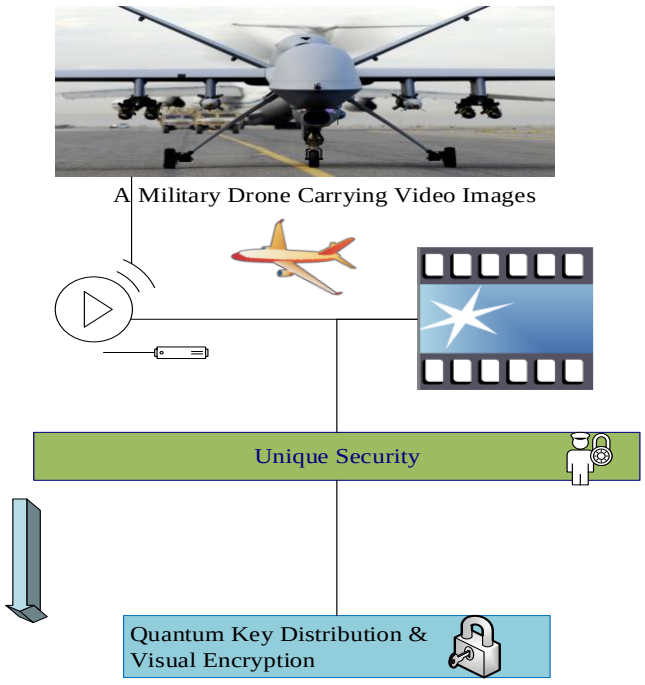

Figure 4. Quantum Key Distribution and VC for security

The security for the sensitive digital images in the cloud environments can be provided by an asymmetric encryption algorithm [26]. The extra security can be provided by implementing visual cryptography in the context. The encryption key is generated from the public key exchange algorithm. Substitution cipher and random grid mechanism is used in connection with visual cryptography for providing enhanced security for the data that is transmitted [27]. It is a two-step encryption process in which in the first step a Caesar cipher is implemented to encrypt the image row wise. Column wise encryption is done with a key of size which is equal to the greatest common divisor of no. of rows and columns in secret image. Finally a generated random matrix is XORed with the transformed secret image.

The concept of Region Incrementing Visual Cryptography (RIVC) was presented by R Z Wang in his research paper [28]. But this concept suffers from pixel expansion issue also with color reversal issues. An enhanced RIVC was introduced which has no pixel expansion problems and with a good increased contrast. This also eliminates the color reversal problems. There were two types of visual cryptographic schemes introduced, former a deterministic visual cryptography by Naor and Shamir and the latter is random grid visual cryptography by Kafri and Keren. A relationship have been found between these two models, meaning any deterministic method would correspond to a random grid method and vice versa is also true [29]. This relationship helps in finding new methods and exploiting their performance evaluations in connection with the other methods. For gray scale images, the visual secret sharing have been proposed by Chen. The process of the same is as follows, random grid method is applied to the sub images which are the resultants of linear equations of Hill cipher. The random grid method is used as a second layer of security for the data. However this methodology has some drawbacks with respect to coefficient matrix used in Hill cipher equations. In order to overcome this issue a new approach on the linear equations have been introduced which is effective and more secure than the other methods [30]. Cheating prevention of information hiding was introduced using two related techniques namely Steganography and Visual Cryptography (VCS) [31]. The VCS distributes the visual information into ‘n’ secret shares. When a message is embedded in to a share, it becomes a stego share. With the help of a hardware module these stego shares are embedded into a cover image. At the receiver end, stego shares are decoded from the cover image first, then secret message is obtained from shares.

The concept of visual cryptographic representations called in short as COALA [32] was developed for educational software system as an additional supplement on Data Security course at the School of Electrical Engineering, University of Belgrade. It helps the students in the university

to perform the calculations by executing various intricate algorithms in a step by step manner. One of the variants in visual cryptography is multi-secret visual cryptography (MVC). The most proficient schemes among MVCs is tagged visual cryptography (TVC) [33]. This scheme has the advantage of maintaining the secrecy of tag images into randomly selected shares. The disadvantage of these MVC schemes and the TVC scheme is that, it has negative effects on the visual quality of the recovered image due to distortion. An extended TVC scheme is proposed to resolve the distortion issues which is named as lossless tagged visual cryptography (LTVC). A probabilistic LTVC (P-LTVC) was also introduced to explain the possible security problems arising in LTVC if any. Visual cryptography in assembly with steganography produces good results for securing the financial online transactions [34]. This method uses these two concepts during online fund transfer with limited information for protecting the customer data over untrusted networks.

To increase the robustness of authentication systems in different organizations, hierarchical visual cryptography (HCV) is applied [35]. HVC takes the signature of an employee and divides them into four shares using base visual cryptographic technique in a hierarchical manner, where in one of the three shares is used for generating key share and other one would be available with the employee. During authentication process, the key share which is available with authentication database gets superimposed with the employees share. If both of the shares syncs with the original partitioned shares, the employee is given permission for access. Visual quality of the grayscale images is improved related to size invariant VCS via Analysis by Synthesis approach [37, 38]. Collaborative visual cryptography schemes provide researchers a newer way of understanding the security solutions [39].

III. VISUAL ENCRYPTION FRAMEWORK FOR PROVENANCE SECURITY

The systems security plays a key role in all the domain areas related to computer science engineering and information technology. Data larceny, security breaches, zero day exploits etc., are still in place despite efficient security mechanism deployed. So, the challenge lies in minimizing these attacks by building robust and hybrid approaches with the help of existing algorithms.

The idea is to provide this unique notion of visual encryption mechanism for a conception named Data Provenance [40]. The lineage of objects over web, which is the provenance of the same is in need of efficient security mechanisms for protection. In the communal platforms importance for the same has grown in recent years as data in web is increasing enormously with rapid rate on regular basis. The protection for objects should be provided with the three perspectives of security fundamentals namely confidentiality, integrity and availability. To achieve this, foundational models should be created to meet the above mentioned security goals.

The problem definition for the assortment of data provenance and visual cryptography is as follows, "Converging on the aspects of visual cryptography which can act as robust security approach for shielding the provenance of an object in the untrusted computer networks to solve many of the real world problems in various domains"[41 42].

IV. RESULTS AND DISCUSSION

An application in this regard is developed and analysis on the same is made with parameters such as one time password, customer Id, timestamp of logging into the tool. Results in connection with these parameters are plotted and are shown below. A five digit random number is the format of one time password. This is basically provided to the user for entry into the provenance based application. Timestamp data is collected with regards to users entry into the system during a particular period. Corresponding customer Id is also captured here. This captured information will be useful in cyber-attack investigations, troubleshooting, risk management etc.

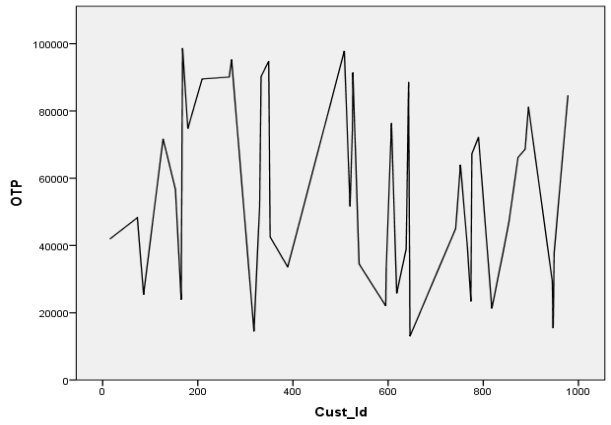

Figure 5. Line graph representation of OTP and Cust_Id

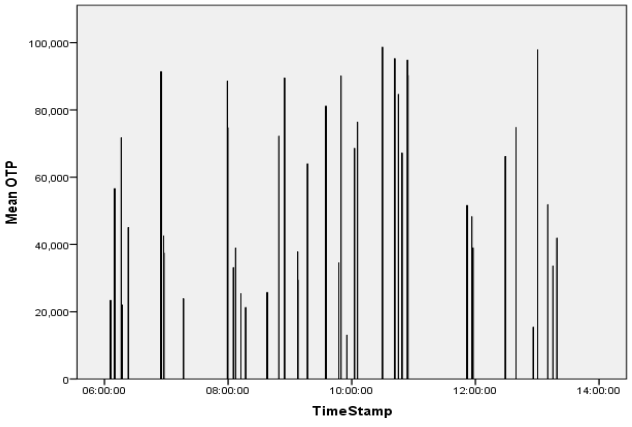

Figure 6. Bar Graph representation of Timestamp Vs Mean of OTP

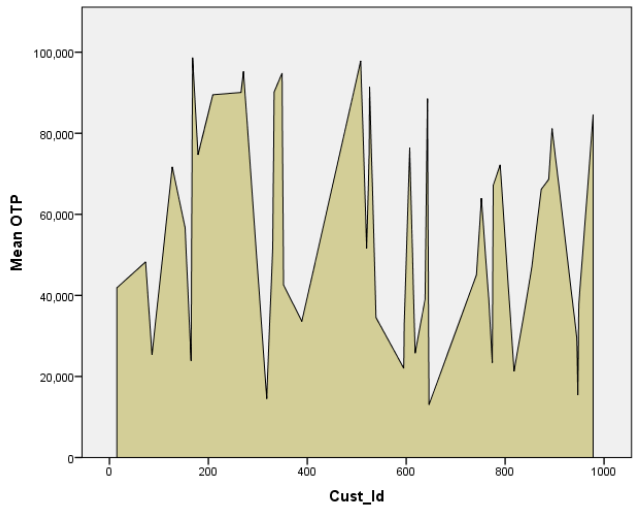

Figure 7. Areaplot representation of Cust_Id Vs Mean of OTP

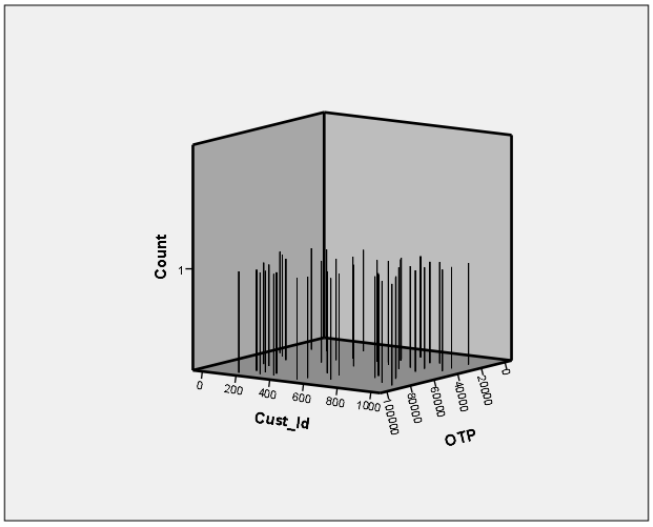

Figure 7. 3-D bar representation of OTP Vs Cust_Id with count parameter

Figure 5. illustrates the line graph representation between OTP and Cust_Id. Timestamp across Mean values of OTP is reflected in Figure 6. Areaplot representation between Cust_Id and Mean OTP is shown in Figure 7. 3-D bar representation of OTP Vs Cust_Id with regards to count parameter is depicted in Figure 8. However these results shows that the parameters selected for data provenance application have no correlation with their numberical values. Their variation can be observed in the above mentioned garphical representation. The recorded results helps in knowing the identity in accessing the system. It helps in troubleshooting issues in cyber attack scenarios. Perhaps the tracking of this lineage corresponds to the defintion of data provenance in the digital world.

V. CONCLUSION

This paper finds a profound knowledge on the aspects of a unique encryption mechanism which uses images for enciphering the information; and human vision for the deciphering process when the correct image key is processed. Various approaches and techniques towards visual cryptography have been discussed and elaborated with relevant information through pictorial representations. The literature study mentioned in the paper starts with description on basic visual cryptography. The paper also gives a brief analysis of all applications developed using visual cryptography. It also throws light on traits associated to secured shared communications. As a note, it delivers the framework for security with regards to a unique research arena named data provenance with associated application development and corresponding results.

REFERENCES

[1] Jithi, P. V., & Nair, A. T. (2013, March). Progressive visual cryptography with watermarking for meaningful shares. In *Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on* (pp. 394-401). IEEE.

[2] Basavegowda, R., & Seenappa, S. (2013, April). Electronic Medical Report Security Using Visual Secret Sharing Scheme. In *Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on* (pp. 78-83). IEEE.

[3] Pope, C., Kaur, K.: 'Is it human or computer? Defending e-commerce with CAPTCHAs', IT Professional, 2005, 7, (2), pp. 43–40

[4] CAPTCHA: Telling Humans and Computers Apart Automatically. Available at: http://www.captcha.net/

[5] Lee, J. S., & Hsieh, M. H. (2013). Preserving user-participation for insecure network communications with CAPTCHA and visual secret sharing technique.*IET networks*, *2*(2), 81-91.

[6] Wu, X., & Sun, W. (2013). Generalized random grid and its applications in visual cryptography.

[7] Zhong, G. S., & Wang, J. J. (2013, May). Region incrementing visual secret sharing scheme based on random grids. In Circuits and Systems (ISCAS), 2013 IEEE International Symposium on (pp. 2351-2354). IEEE.

[8] Yang, Ching-Nung, and Daochun Wang. "Property Analysis of XOR Based Visual Cryptography." (2014): 1-1.

[9] Daoshun, W., et al. "Optimal Contrast Greyscale Visual Cryptography Schemes with Reversing." (2013): 1-1.

[10] Chiu, P. L., Lee, K. H., Peng, K. W., & Cheng, S. Y. (2013, July). User-friendly visual cryptography with complementary cover images. In *Signal and Information Processing (ChinaSIP), 2013 IEEE China Summit & International Conference on* (pp. 641-644). IEEE.

[11] Tan, X., & Zhang, Q. (2013, September). A Kind of Verifiable Visual Cryptography Scheme. In Emerging Intelligent Data and Web Technologies (EIDWT), 2013 Fourth International Conference on (pp. 215-219). IEEE.

[12] Iwamoto, M. (2012). A weak security notion for visual secret sharing schemes. Information Forensics and Security, IEEE Transactions on, 7(2), 372-382.

[13] Premkumar, S., & Narayanan, A. E. (2012, March). New visual Steganography scheme for secure banking application. In *Computing,*

Electronics and Electrical Technologies (ICCEET), 2012 International Conference on (pp. 1013-1016). IEEE.

[14] Lin, K. T. (2012, July). Based on Binary Encoding Methods and Visual Cryptography Schemes to Hide Data. In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on (pp. 59-62). IEEE.

[15] Surekha, B., Swamy, G., & Reddy, K. R. L. (2012, July). A novel copyright protection scheme based on Visual Secret Sharing. In *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on* (pp. 1-5). IEEE.

[16] Prema, G., & Natarajan, S. (2013, February). Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application. In *Information Communication and Embedded Systems (ICICES), 2013 International Conference on* (pp. 727-730). IEEE.

[17] W.P. Fang and J.C. Lin, "Visual cryptography with extra ability of hiding confidential data," Journal of Electronic Imaging , Vol. 15, No. 2, pp.0230201–023020 7, 2006.

[18] Huang, Y. J., & Chang, J. D. (2013, February). Non-expanded visual cryptography scheme with authentication. In *Next-Generation Electronics (ISNE), 2013 IEEE International Symposium on* (pp. 165-168). IEEE.

[19] Kaur, K., & Khemchandani, V. (2013, February). Securing Visual Cryptographic shares using Public Key Encryption. In *Advance Computing Conference (IACC), 2013 IEEE 3rd International* (pp. 1108-1113). IEEE.

[20] Lee, K., and P. Chiu. "Image size invariant visual cryptography for general access structures subject to display quality constraints." (2013): 1-1.

[21] Babu, C. R., Sridhar, M., & Babu, B. R. (2013, March). Information hiding in gray scale images using pseudo-randomized visual cryptography algorithm for visual information security. In *Information Systems and Computer Networks (ISCON), 2013 International Conference on* (pp. 195-199). IEEE.

[22] Rajendra, A. B., & Sheshadri, H. S. (2013, August). Visual Cryptography in Internet Voting System. In *Innovative Computing Technology (INTECH), 2013 Third International Conference on* (pp. 60-64). IEEE.

[23] Lee, K., and P. Chiu. "Digital Image Sharing by Diverse Image Media." (2014): 1-1.

[24] Liu, X. Y., Chen, M. S., & Zhang, Y. L. (2013, August). A new color visual cryptography scheme with perfect contrast. In *Communications and Networking in China (CHINACOM), 2013 8th International ICST Conference on* (pp. 449-454). IEEE.

[25] Kester, Q. A., Nana, L., & Pascu, A. C. (2013, November). A novel cryptographic encryption technique of video images using quantum cryptography for satellite communications. In *Adaptive Science and Technology (ICAST), 2013 International Conference on* (pp. 1-6). IEEE.

[26] Kester, Q. A., Nana, L., & Pascu, A. C. (2013, November). A new hybrid asymmetric key-exchange and visual cryptographic algorithm for securing digital images. In *Adaptive Science and Technology (ICAST), 2013 International Conference on* (pp. 1-5). IEEE.

[27] Yadav, G. S., & Ojha, A. (2013, December). A novel visual cryptography scheme based on substitution cipher. In *Image Information Processing (ICIIP), 2013 IEEE Second International Conference on* (pp. 640-643). IEEE.

[28] Thankappan, A., & Wilscy, M. (2013, December). (2, 3) RIVC Scheme in Visual Cryptography without Pixel Expansion. In *Advanced Computing, Networking and Security (ADCONS), 2013 2nd International Conference on* (pp. 259-263). IEEE.

[29] De Prisco, R., & De Santis, A. (2014). On the Relation of Random Grid and Deterministic Visual Cryptography. *IEEE transactions on information forensics and security*, *9*(3-4), 653-665.

[30] Bunker, S. C., Barasa, M., & Ojha, A. (2014, February). Linear equation based visual secret sharing scheme. In *Advance Computing Conference (IACC), 2014 IEEE International* (pp. 406-410). IEEE.

[31] Jana, B., & Jana, S. (2014, February). Cheating prevention in Visual Cryptographic Schemes using message embedding: A hardware based practical approach. In *Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on* (pp. 319-324). IEEE.

[32] Stanisavljevic, Zarko, et al. "COALA-System for Visual Representation of Cryptography Algorithms." 1-1.

[33] Wang, Xiang, Qingqi Pei, and Hui Li. "A Lossless Tagged Visual Cryptography Scheme." (2014): 1-1.

[34] Roy, S., & Venkateswaran, P. (2014, March). Online payment system using steganography and visual cryptography. In *Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on* (pp. 1-5). IEEE.

[35] Chavan, P. V., Atique, M., & Malik, L. (2014, March). Signature based authentication using contrast enhanced hierarchical visual cryptography. In*Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on* (pp. 1-5). IEEE.

[36] M. Naor and A. Shamir, "Visual Cryptography," Advances in Cryptography: Eurocrypt'94, Springer-Verlag, Berlin, pp. 1-12.

[37] Yan, B., Xiang, Y., & Hua, G. (2019). Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach. *IEEE Transactions on Image Processing*, *28*(2), 896-911.

[38] Yang, C. N., Wu, C. C., & Lin, Y. C. (2017). k out of n Region-Based Progressive Visual Cryptography. *IEEE Transactions on Circuits and Systems for Video Technology*.

[39] *Jia, X., Wang, D., Nie, D., & Zhang, C. (2018). Collaborative visual cryptography schemes. IEEE Transactions on Circuits and Systems for Video Technology, 28(5), 1056-1070.*

[40] I. M. Yazici, E. Karabulut and M. S. Aktas (2018), "A Data Provenance Visualization Approach," *2018 14th International Conference on Semantics, Knowledge and Grids (SKG)*, Guangzhou, China, pp. 84-91

[41] Kumar, K. P., & Cherukuri, R. C. (2016, May). The secured data provenance: Background and application oriented analysis. *In 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 1212-1216). IEEE.

[42] Kumar, K. P., & Cherukuri, R. C. (2018, July). Secured Electronic Transactions Using Visual Encryption: An E-Commerce Instance. In *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 1341-1345). IEEE.

