ENCRYPTED DATA HIDING IN CRYPTOGRAPHY PROCESS USING KEYLESS ALGORITHM

[1]M.Jayabharathi,[2]M.Harikrishnan.M.Tech.,
[1]Pursuing M.E, Dept of CSE
[2]Assistant Professor, Department of Computer Science and Engineering

Abstract: Securing data is a challenging issue in today's technology. Most of the data travel over the internet and it becomes difficult to make data secure. The information security has become one of the most major problems in data communiqué. So it becomes an inseparable part of data communication. In order to address this problem, cryptography technique is used for data transmission to making data secure. There arises a need of data hiding. So here we are using a combination of steganography and cryptography for improving the security. All previous methods insert data by random vacating room from the encrypted images, which may be subject to some errors on data extraction and image re-establishment.

Keywords~~O~~pinion:Extraction, Owner side Encryption the data using keyless algorithm

I. INTRODUCTION

The main trait of the encryption/decryption program accomplishment is the generation of the encryption key. Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space difficulty

II. RELATED WORK

2.1 CUSTOMER TRANSACTION POINTS

Security cameras should also be placed at any point of customer transaction.This includes cash registers, teller stations and kiosks. Next to entrances and exits, these areas afford your best chance of capturing investigative images. Try to keep these cameras about 7 feet high and looking directly into the area. If you mount the

cameras too high (on the ceiling, for example) you won't see anything but the tops By targets, I'm referring to cash drawers, jewelry cabinets, safes, filing cabinets or any area that a thief may target. In these areas, you want your security cameras to capture as wide an image as possible. The idea here is not so much to identify a face as it is to review or respond to a crime. These are also areas where security cameras may be mounted relatively high so that they can see down into cabinets and drawers. [14] Parking lots and back alleys are also useful locations for security cameras. The images you capture in these areas are useful for investigating vandalism or violence. The deterrent value of your camera system also comes into play in these applications.In addition to customer review texts, opinion target extraction has been conducted on open-domain texts such as newsIII. articles. Kim and Hovy [12] used semantic role labeling as an intermediate step to label opinion holder and target. They utilized FrameNet data to get annotated corpus by mapping target words to opinion-bearing words and mapping semantic roles to holders and targets. Ma and Wan [16] A reversible or lossless watermarking algorithm for images without using a location map in most cases. This algorithm employs prediction errors to embed data into an image. A sorting technique is used to record the prediction errors based on magnitude of its local variance. Using sorted prediction errors and, if needed, though rarely, a reduced size location map allows us to embed more data into the image with less distortion. The performance of the proposed reversible watermarking scheme is evaluated using different images and compared with four methods. The results clearly indicate that the proposed scheme can embed more data with less distortion. often comes at the expense of image fidelity. Most watermarking techniques modify, and hence distort, the host signal in order to insert authentication information. In many applications, loss of image fidelity is not prohibitive as long as original and modified images are perceptually equivalent. On the other hand, in medical, military, and legal imaging applications, where the need for authentication is often paramount, there are typically stringent constraints on data fidelity that prohibit any permanent signal distortion in the watermarking process.

earlier methods, the LAW framework validates the images before attempting to reconstruct the original image. As a result, the image reconstruction step may be skipped when either a) the verification step fails, or b) the watermarked image meets the quality criteria and the perfect original is not needed. The computational savings are often substantial due to the complexity of the reconstruction step. Computational advantages in the embedding phase. In client/server applications where a single image is served to multiple clients with different signatures (or time-stamps), the LAW framework has additional computational advantages. In this case, the server performs the—often costly—pre-embedding step only

once and inserts different signatures as requested by clients.

III PUBLIC/PRIVATE-KEY SUPPORT

The LAW framework also supports the public-validation/private-recovery property of [16], without the need for a second signature. When a public-key authentication signature is used in conjunction with a private-key dependent lossless watermark, the framework supports public validation of the watermarked image, but limits access to the perfect original.

approach. Kim and Zhai [22] proposed the contrastive opinion summarization problem. They aim to find reviews that have opposite senti- ment orientations on the same aspect. The task is formu- lated as an optimization problem and two general methods are proposed for generating a comparative summary using the content similarity and contrastive similarity of two sen- tences. Lu et al. [23] ordered aspects and their correspond- ing sentences based on a coherence measure, which tried to optimize the ordering so that they could best follow the sequences of aspect appearances in their original posting. In addition to review summarization,opinion summari- zation has been applied on microblogs recently. Weng et al. [24] presents a system to summarize a microblog post and its responses with the goal to provide readers with a more constructive and concise set of information for efficient digestion. They proposed a novel two-phase summarization scheme. In the first phase, the post plus its responses are classified into one of the following four categories, interro- gation, sharing, discussion and chat. Opinion analysis is then used to classify the polarity of the sharing and discus- sion posts. Bora [25] built a sentiment classification tool which is used to analyze a collection of tweets. They give the opinion distribution to of the tweets retrieved by a given query as the summary. Meng et al. [26] also dealt with the opinion summarization problem for a given entity. After getting the tweet collection which contains the entity, they extract the subtopics from all the hashtags in the tweets. Each subtopic can be represented by several hashtags. For each subtopic, a classifier is used to find insightful tweets which not only convey opinions but also provide insight. They also build a SVM-based classifier to find target-depen- dent opinions. It is worth noting that the task of [26] is dif- ferent from ours. In their framework, the targeting corpus is the tweet collection retrieved by an entity. They extract dif- ferent hashtags as subtopics from the tweet collection and summarize the opinion towards these topics. On the receiver side, the watermark verification and recovery are performed as illustrated . The process begins by overlaying the grid of image blocks (at the lowest level of the hierarchy) over the image pixels which allows the determination of the parts and that carry authentication information and image information, respectively (as seen in Fig. 4). The (presumed) authentication information from bits constituting part (the LSBs corresponding to

shaded regions in Fig. 4) is then extracted and these bits are reset to zero in the image. If the received image is exactly the watermarked image (no alterations), this process recovers the pre-embedded image that was produced at the embedder. Next, the quad-tree hierarchy of Fig. 6 is overlaid on the image blocks (and the corresponding extracted authentication information) to compute signatures corresponding toeach of blocks in the hierarchy and validate these against the signatures already extracted from part .

It is accepted that digital watermarking is quite relevant in medical imaging. However, due to the special nature of clinical practice, it is often required that watermarking not introduce irreversible distortions to medical images. The electronic clinical atlas has such a need of "lossless" watermarking. We present two tailored reversible watermarking schemes for the clinical atlas by exploiting its inherent characteristics. We have implemented the schemes and our experimental results look very promising.marked signal is obtained by quantization. Quantization watermarks suffer from low robustness, but have a high information capacity due to rejection of host interference.

3.1 SYSTEM OVERVIEW

A content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider. The data hider can embed some auxiliary data into the encrypted image by randomly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key, But alone cryptographycannot provide a better security approach because the scrambled message is still available to the eavesdropper.

IV. PROBLEM STATEMENT

Existing system VRAE the cloud server embeds data by losslessly vacating room from the encrypted images by using the idea of compressing encrypted images. Compression of encrypted data can be formulated as source coding with side information at the decoder. Usually the side information is the correlation of plaintexts that is exploited for decompression by the decoder. In divided the encrypted image into several blocks. By flipping 3 LSBs (least significant bits) of the half of pixels in each block, room can be vacated for the embedded bit. The data extraction and image recovery proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in the decrypted image. Other framework RRBE the image owner first empties out room by using RDH method in the plain images. After that, the image is encrypted and outsourced to the cloud and the cloud server can freely embed data into the reserved room of the encrypted image. The first method under RRBE framework was presented

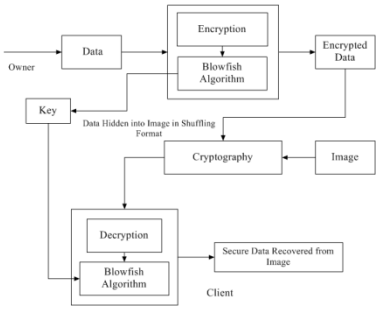
in which reserves room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypts the image, so the positions of these LSBs in the encrypted image can be used to embed data.

V. SYSTEM MODEL

A.PROPOSED SYSTEM

We propose Cryptography is the art of achieving security by encoding the data into unreadable form. Data thatcan be unreadable and not understood with difficulty is called encryption cryptography. Proposed processshufflingthe data image pixels from the encrypted images is relatively difficult and sometimes inefficient, If we shuffling the order of encryption and vacating room prior to image encryption at content owner side with a traditional Keyless algorithm, and thus it is easy for the data hider to shuffling embed data in the encrypted image. Encrypted images would be more natural and much easier which leads us to the novel framework for secure data transmission.

We propose cipher after encrypting the entire data of uncompressed form, we can embed theadditional data into an image by modifying a small proportion of an image. Once data isencrypted and sent, the receiver can decrypt thedata by using encryption key. The decryptedimage is similar to the original image. The embeddeddata can be extracted by using the data-hiding key and original image is recovered back.First to transform the content of original image into the content of another target image with the same size. The transformed image that expressions comparable the target image is used as the encrypted image and is subcontracted to the cloud. Then, the cloud server container simply embed data into the “encrypted image” by any RDH methods for plaintext images. Traditional RDH scheme and unified embedding and scrambling scheme, are adopted to embed watermark in the encrypted image.



SYSTEM ARCHITECTURE

A generic discipline to handle objects (existing or to be created) called "systems", in a way that supports reasoning about the structural properties of these objects. Systems Architecture is a response to the conceptual and practical difficulties of the description and the design of complex systems.

SUPPORT ENCRYPTED IMAGE TO CLOUD

Cloud encryption is the transformation of a cloud service customer's data into cipher text. Cloud encryption is almost identical to in-house encryption with one important difference -- the cloud customer must take

time to learn about the provider's policies and procedures for encryption and encryption key management. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted. encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century." It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques.

The selection process to find this new encryption algorithm was fully open to public scrutiny and comment; this ensured a thorough, transparent analysis of the designs. Conventionally, data embedding techniques aim at maintaining high-output image quality so that the difference between the original and the embedded images is imperceptible to the naked eye. Recently, as a new trend, some researchers exploited reversible data embedding techniques to deliberately degrade image quality to a desirable level of distortion. In this paper, a unified data embedding-scrambling technique called UES is proposed to achieve two objectives simultaneously, namely, high payload and adaptive scalable quality degradation. First, a pixel intensity value prediction method called checkerboard-based prediction is proposed to accurately predict 75% of the pixels in the image based on the information obtained from 25% of the image.

CONCLUSION AND FUTURE WORK

Security in the Internet is improving. The increasing use of the Internet for trade is improving the deployed technology to protect the financial business Extension of the basic technologies to protect multicast communications is possible and can be expected to be deployed as multicast becomes more widespread. Control over routing remains the basic tool for controlling access based on the keyless algorithm. implement particular policies will be possible as multicast routing protocols improve. Cryptography is a tool which may alleviate many of the perceived problems of using the Internet for communications. Our method is essentially to secure communication method and it will take less time if the file size is large. The important thing of our proposed method is that it is almost impossible to break the encryption algorithm without knowing the exact key value. In future method, encryption method with keyless algorithm can be applied for data encryption and decryption in any type of public application for sending top secret data.

REFERENCES

[1] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," Phys. Rev. Lett., vol. 71, no. 1, pp. 65–68, 1993.

[2] K.M.Cuomo,A.V.Oppenheim,andS.H.Strogatz," Synchronization ofLorenz-basedchaoticcircuitswithapplicationstocommunications," IEEETrans.CircuitsSyst.II,AnalogDigit.SignalProcess.,vol.40,pp. 626–633, 1993. [3] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fisher, J. Garcia-Ojarvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-basedcommunicationsathighbitratesusingcommercialfibre- optic links," Nature, vol. 437, pp. 343–346, 2005.

[4] H. Dedieu, M. Kennedy, and M. Hasler, "Chaos shift keying: Modu- lation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process., vol. 40, pp. 634–642, 1993.

[5] S. Hayes, C. Grebogi, E. Ott, and A. Mark, "Experimental control of chaos for communications," Phys. Rev. Lett., vol. 73, pp. 1781–1784, 1994.

[6] Y. Lai, E. Bolt, and C. Grebogi, "Communicating with chaos using two-dimensional symbolic dynamics," Phys. Lett. A, vol. 255, pp. 75–81, 1999.

[7] T. Miyano, K. Nishimura, and Y. Yoshida, "Chaos-based communi- cations using open-plus-closed-loop control," IEICE Trans. Fundam., vol. E94-A, pp. 282–289, 2011.

[8] R. Tenny, L. S. Tsimring, L. Larson, and H. D. I. Abarbanel, "Using distributed nonlinear dynamics for public key encryption," Phys. Rev. Lett., vol. 90, pp. 047903-1–047903-4, 2003.

[9] R. Tenny and L. S. Tsimring, "Additive mixing modulation for public key encryption based on distributed dynamics," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 52, no. 3, pp. 672–679, 2005.

[10] L. Kocarev, M. Sterjev, A. Fekete, and G. Vattay, "Public-key encryp- tion with chaos," Chaos, vol. 14, no. 4, pp. 1078–1082, 2004.

[11] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: From theory to practical algorithms," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 53, no. 6, pp. 1341–1352, 2006.

[12] F. Anstett, G. Millerioux, and G. Bloch, "Chaotic cryptosystems: Cryptanalysis and Indentifiability," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 53, no. 12, pp. 2673–2680, 2006.