A Review Paper on Securing Surveillance Data using Incremental Cryptography

Lissiyas Antony
Student, Master of Technology
Computer Science and Engineering
Rajiv Gandhi Institute of Technology (Government Engineering College, Kottayam)

Dr. Sobhana N V
Professor, Dept. of Computer Science and Engineering
Rajiv Gandhi Institute of Technology (Government Engineering College, Kottayam)

***Abstract*— Major cryptographic primitives like signatures and encryption have considerably received a significant theoretical treatment. In different works, the definition of privacy and security has extensively been emphasized, proposed, and attained. In this study, prospects of incremental cryptography are emphasized to understand how it helps to secure surveillance data. When securing surveillance data, incremental cryptography provides practical operation like update here one can take advantage of the well-known fact that successive video frames usually differ only slightly. To attain incrementally for efficient encryption of data, different tools such as byte-wise incremental encryption, and incremental SHA-3 and MAC are used for encryption. Besides, for the security of encrypted surveillance data, one of the conditions to meet is the parallelizability for decryption and encryption, and that the nonce should be iterated severally.**

Keywords—Incremental Cryptography, Image Encryption, Encryption, security, Real time surveillance

I. INTRODUCTION

Image encryption is critical for ensuring secure image transmission and capacity over the internet. A real-time image encryption, on the other hand, faces a more significant challenge due to the large amount of data involved. Surveillance becoming an integral part of our security infrastructure, privacy rights are beginning to gain importance. Wireless multimedia surveillance networks are part of IoT-assisted environment, which consists of visual sensors that observe the surrounding environment by continuously capturing images, thereby producing a large amount of visual data with significant redundancy. Sending all the imaging data through the communication lines without processing is impractical and the encryption which is comparatively difficult and time-consuming. Therefore is is very necessary to implement an encryption system which provides a security and less encryption time

Incremental cryptography [11] designs cryptographic algorithms with the aim that, by applying an algorithm to the data or document possible to update the algorithm’s document for the modified document instead of re-computing it from scratch. A document or data that undergoes cryptographic transformation doesn’t exist in isolation, rather it is constructed from other already transformed documents. Therefore, in emphasizing the impact of incremental cryptography, Bellare, Goldreich & Goldwasser affirm that in cases where different forms of cryptographic algorithms like signatures and encryption are applied to the changing data like the surveillance data which is prone to changes, efficiency improvements are often achieved. As the three authors maintain, such kind of setting is using authentication tags to protect documents from viruses [9]

II. LITERATURE REVIEW

A. *Incremental Cryptography*

Mihir Bellare et al., [1]. They are the first to investigate a new type of cryptographic transformation efficiency. The notion is that once a transformation has been applied to a document M, the time it takes to update the result when M is modified should be "proportional" to the "amount of alteration" done to M. As a result, considerably faster cryptographic primitives for environments are obtained.

Mihir Bellare, Daniele Micciancioy [2] proposed a novel, straightforward paradigm for creating collision-free hash functions. Any function that emerges from this paradigm is a step forward. (This indicates that if a message X which I have previously hashed is modified to X (0), so instead of Recalculating the hash of X (0) from the ground up, we can swiftly upgrade the old hash value to the new one. They introduce a new paradigm for the construction of collision-free hash functions

Subodha Charles and Prabhat Mishra,[3] proposed a light weight security mechanism that increases the performance of existing encryption algorithms used in NoC while consuming very little space and power. The encryption/decryption in the security architecture ensures secure communication on the NoC They used incremental encryption to improve performance by utilizing the unique traffic characteristics of packets observed in an NoC. Also their framework better in terms of security to prove that the performance gain is not achieved at the expense of security. Experimental results show a performance improvement in encryption time and in total execution time compared to traditional encryption while introducing less than 2% overall area overhead.

B. *Image encryption techniques*

Quist-Aphetsi Kester,[5] Proposed Image Encryption based on the RGB PIXEL Transposition and Shuffling 2013. This paper suggested a technique of transposition and reshuffling of the RGB values of the image in steps, which has proven to be really effective in terms of security analysis. The extra swapping of RGB values in the image file after RGB component shifting has increased the security of the image against all possible attacks that are currently available.

P. Junwale et al., [4] suggested a block-based technique for image security Techniques for picture modification and Hyper Image Encryption The original image was broken into blocks, which were then combined to create a new image. Were reconstructed using a transformation algorithm into a converted image, and then the converted image was encrypted using the Blowfish algorithm. Encryption algorithms for hyper images to put it another way, the correlation between image parts was dramatically reduced as a result of the experiment. Their findings also revealed that employing smaller block sizes to increase the number of blocks resulted in lower correlation and higher entropy. There is no key generator in this algorithm. The image was divided into a number of parts using the Hyper Image encryption technique. Due to the large data size and real time constrains. Algorithms that are good for textual data may not be suitable for multimedia data. In this algorithm the correlation between image elements was greatly reduced using this technique.

W. Zhu, [7] developed a novel method for image discretization that leverages Cat mapping. Periodic adjustments are used in the suggested methodology to produce image encryption. Images containing Encryption cycles may differ depending on the size of the object. Experiments show that the encryption method is effective. This approach is capable of performing effectively on image pixel scrambling and replacement, according to the sensitivity analysis. For encrypted security, this proposed method has strong sensitivity to the plaintext which may attribute to handle the plaintext attack under difference situations.

Bibhudendra Acharya et al., [8] proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption. The goal of this study is to address the disadvantage of utilising a random key matrix for encryption in the Hill cypher technique. Where we may not be able to decrypt the encrypted message, if the key matrix is not invertible. Additionally, by skipping the process of obtaining the inverse of the matrix during decryption, the computational cost can be decreased, as they use Involutory key matrix for encryption. They used this key matrix to encrypt both grayscale and colour images. The algorithm works well for all types of gray scale as well as color images except for the images with background of same gray level or same color.

III. HOW TO SECURE SURVEILLANCE DATA USING INCREMENTAL CRYPTOGRAPHY

Bellare, Goldreich & Goldwasser further hold that when encrypting sensitive documents or files like the surveillance data in our case, once a file has been encrypted, minor changes can be done on such an original file [9]. Incremental encryption serves a critical impact in different situations. One of the scenarios involves updating obfuscated code so that video transmission of images and patches are accommodated [10]. In such a scenario, incremental encryption helps to find “the cryptographic transformation of a modified input not from scratch but as a function of the encrypted version of the input from which the modified input was derived. When the changes are small, the incremental method gives considerable improvements in efficiency. [3]

In early days, the focus of incremental cryptography was on signature, MAC and hashing and Encryption on documents [1]. Incremental encryption on video traffic has never been discussed. Here one can take advantage of the well-known fact that successive video frames and images usually differ only slightly. The main focus here is on lowering encryption time while maintaining the same level of security as current encryption algorithms.

The introduced scheme provides a fully encryption technique that is used in the surveillance data since all information is hidden instead of encrypting or decrypting particular portion of data. This means that, a better security with optimal computational time can be attained.

IV. REDUCING COMPUTAIONAL TIME OF SURVEILLANCE DATA USING INCREMENTAL CRYPTOGRAPHY

Huge amount of data in the real-time surveillance causes a high computational time, mostly when one uses the traditional encryption scheme. Therefore, to reduce the encryption time of the surveillance data, incremental encryption is proved more

When encrypting successive images or frames, the first image is encrypted from scratch using the existing system, and the subsequent images are compared with previous frames to determine the index of the changed portion, and encryption can then be performed on the required portion. The comparison factor must be determined by the user. Because of the image data, we are unable to use all encryption algorithms. By establishing a criterion for comparison we can figure out how much has changed.

An incremental cryptographic [11] scheme can be specified by the quad S = (kGen, E, D, Inc) of probabilistic, polynomial time algorithms.

A. Key Generator KGen

Which yields the secret key k

B. Encryption Algorithm

Takes as input a key K, and an image I. It outputs an encrypted Image

$$C = E(K, I) = E_k(I) \quad (1)$$

C. Decryption Algorithm :

Takes as input a cipher image C, and outputs a decryption of it

$$M = D(K, C) = D_k(C). \quad (2)$$

D. Incremental Algorithm

Takes as input a key K, and old imageI_{old}, and instructions on how to change the document (old =. new). It yields a new ciphertext

$$C_{new'} = Inc_k(I_{old}\ (\text{old} \Rightarrow \text{new})) \quad (3)$$

V. APPLICATIONS OF INCREMENTAL CRYPTOGRAPHY

Aside from employing incremental cryptography to dynamically produce signatures, encryptions, and MACs, there are other options.[11] Many more real-world applications can benefit from incremental cryptography.

A. Filesystems

Within Filesystems, incremental cryptography is used as a kind of virus protection or data protection. Filesystem research has revealed patterns among certain paths. Some files are transient files that are generated and erased in their entirety, while others are primarily appended to. Finally, there are files that have had appends, modifications, and deletions made to them.

B. Webpage

Many sorts of web services now desire to encrypt data sent over the internet. Many of the objects that are transferred are static pages (such as an online dictionary), but others are not. Many websites include shopping carts that you can fill with items, allowing you to add one item at a time. There are also sites with fill-in forms. Both of these features appear to be perfect for incremental encryption

C. Electronic Cash

Many techniques for conducting business through the Internet have been proposed. Some are based on the concept of an electronic wallet that the user carries about with him or her and that changes after each transaction. Digital signatures are used to ensure that the user is verified and that the wallet is valid in the eyes of the bank. Because most wallet modifications are in the form of "add cash" or "delete cash" incremental cryptography might be utilized here as well.

VI. CONCLUSION

Incremental cryptography has been shown to be particularly effective in both decreasing user-visible delays and embedding cryptography deeper inside applications. It does, however, represent a significant step toward a long-term solution to the concerns of simplicity of use, perceived speed, and integration. Also, incremental encryption which helps to reduce the encryption time for large amount data mainly in the surveillance section

REFERENCES

[1] Mihir Bellare, O. Goldreich and S.Goldwasser, ”Incremental Cryptography: The Case of Hashing and Signing”, Crypto., Mar. 1994.

[2] M. Bellare and D. Micciancio, “A new paradigm for collision-free hashing: Incrementality at reduced cost, EUROCRYPT 1997: Advances in Cryptology — EUROCRYPT ’97 pp 163-192 http://www-cse.ucsd.edu/users/mihir.

[3] S. Charles and P. Mishra, "Securing Network-on-Chip Using Incremental Cryptography," 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2020, pp. 168-175, doi: 10.1109/ISVLSI49217.2020.00039.

[4] P. Junwale, R. M. Annapurna, and G. Sobha, "A Review on Image Encryption Technique based on Hyper Image Encryption Algorithm," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 11, pp. 614-618, November – 2013

[5] Kester, Quist-Aphetsi. (2013). Image Encryption based on the RGB PIXEL Transposition and Shuffling. International Journal of Computer Network and Information Security. 5. 43-50. 10.5815/ijcnis.2013.07.05.

[6] P. Junwale, R. M. Annapurna, and G. Sobha, "A Review on Image Encryption Technique based on Hyper Image Encryption Algorithm," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 11, pp. 614-618, November – 2013

[7] W. Zhu, "Image Encryption using CAT Mapping and Chaos Approach," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 3, pp.1-8, 2014.

[8] Acharya, Bibhudendra & Panigrahy, Saroj Kumar & Patra, Sarat & Panda, Ganapati. (2009). Image Encryption Using Advanced Hill Cipher Algorithm. International Journal of Recent Trends in Engineering.

[9] Bellare, M., Goldreich, O., Goldwasser, S. (1995). Incremental cryptography and application to virus protection. STOC. Pp. 45–56.

[10] Garg S., Pandey O. (2017) Incremental Program Obfuscation. In: Katz J., Shacham H. (eds) Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science, vol 10402. Springer, Cham. https://doi.org/10.1007/978-3-319-63715-0_7

[11] Yerushalmi, Yoav. (2008). Incremental cryptography.