Three-Level GIS Data Security: Conjointly Cryptography and Digital Watermarking

Monika Bansal and Akanksha Upadhyaya

Abstract Geographic Information System (GIS) plays a vital role in many applications especially in military operations as they need to be spatial in nature. Successful application of military operations demands for accuracy of information and quick decisions taking steps. GIS has now become the most powerful medium for sharing of military information to officers and commanders. In the era of digital communication, officers use GIS to deliver their strategic plans to intended officers [5]. GIS has proven to be an excellent tool for enforcement and deployment of security mechanisms in military applications and to deliver confidential information at distant locations. In our proposed system, we will introduce a new mechanism to protect GIS data carrying confidential and sensitive data for military and army purpose by combining two of the cryptography algorithms: Advanced Encryption Standard (AES) and RSA with digital watermarking techniques.

Keywords GIS · Cryptography · Digital watermarking · AES
RSA

1 Introduction

Experts have long been recognized the importance of GIS in military and commercial application. The GIS data has two important properties. First, the effort it takes to put it in a suitable form for use in the GIS applications. This effort increases its cost. Second, GIS data contains confidential and sensitive information most of the time and it needs to be kept away from unauthorized users. Two possible threats for GIS data are as follows:

M. Bansal (✉) · A. Upadhyaya
Rukmini Devi Institute of Advanced Studies, Delhi, India
e-mail: monikabansal79@gmail.com

A. Upadhyaya
e-mail: akanksha0707@gmail.com

M. U. Bokhari et al. (eds.), *Cyber Security*, Advances in Intelligent Systems
and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_24

1. Illegal duplication and distribution—As GIS data is expensive and sensitive by nature, third parties used to make copies of this data by purchasing some layers of GIS and later sell them without taking any permission from original GIS data provider.
2. Unauthorized access—The act of accessing and tampering of data is done by intruder while information is being transmitted over untrusted communication channel.

The proposed system introduced in this paper is an attempt to solve these security problems in relation to GIS data.

2 Organization of Paper

Paper is organized into seven sections. Section 3 gives applications and limitations of cryptography and digital watermarking. In Sect. 4, we discussed security issues and threats while using GIS data with respect to the past work. We introduced and explained our proposed system with the help of flowchart in Sect. 5. At last, the paper is concluded by its future work.

3 Pros and Cons: Cryptography and Digital Watermarking

Cryptography, digital watermarking, and many other technologies have been used to handle security threats. Each of these technologies has its limitations and has been long used as a weapon to solve security and authentication problems related to data transmitted over network. Both of these have diversified applications and usage with different objectives.

Cryptography tries to take care of three important properties of information including confidentiality, authenticity, and integrity, while it is being transmitted over public network. It is the method of encryption of original data at sender side using key and algorithm before being transmitted over Internet and do reverse of the same process at receiver side. Encryption is the process of converting a readable or meaningful data in an unreadable and meaningless form. Many algorithms like AES, RSA, Hashing, etc. used for the same purpose. It is also used for the purpose of sharing secured data over unsecured network. The efficiency of cryptography depends on key management and its distribution and not on the algorithm used and this is one of the biggest security threats with this technique.

Digital watermarking is the method of hiding a digital information into digital signal like an image, audio, or video signal itself. One of the mostly used applications of digital watermarking is owner identification. To identify the owner of specific image or song, copyright information is embedded in the image or song itself. Other applications of digital watermarking include tampering detection, fingerprinting, broadcast monitoring, etc. [4].

The major limitation of digital watermarking is the manipulation of innocent image including cropping, color variations, rotations, lossy compression, etc. Moreover, some of the features of original image like color, texture, pixel's width, etc. get changed by digital watermarking to embed data or confidential information into it. Changing the features of image distorts the image, and many times it becomes very difficult to recover original image from the distorted image. Also, it cannot protect the GIS data and confidential information from access by unauthorized users.

A more secure system could be built by linking digital watermarking with cryptography. Security can be enhanced for broadcasting of such a sensitive and confidential data like GIS data by this method.

4 Related Work

From the past many years, GIS has been used by government agencies to transfer information. Earlier, professionals used to identify threats, plan resource deployments, and map potential action and contingency plans with the help of GIS. Also, for drawing and printing maps and for building of information desktop, applications were widely used. However, nowadays, the GIS platform allow users the ability to access confidential information and to use of maps in any easy manner in 24 × 7 from anywhere to anywhere and also on any network [3]. Being of its capability to deliver confidential and secret information, GIS is used by military forces in a variety of applications including terrorist activities monitoring, remote sensing, borderlines monitoring, order enforcement at battlefield, etc. The work that has been done in this area is mostly based on digital watermarking [6, 7]. Watermarking is a process of obtaining a digital watermarked file by embedding hidden information (watermarking pattern or watermark for simplicity) like copyright string in a dataset without producing perceptible changes in the data using a suitable watermarking algorithm [1].

5 Proposed System

The proposed algorithm is designed with an objective to provide a method for secure communication of confidential and sensitive information in the form of digital data like images including maps, shape files, etc. along with copyright messages over a network. The proposed model employs digital watermarking with cryptography having two levels of AES and one level of RSA. Several techniques are used for digital watermarking. Our proposed system uses least significant bit embedding technique in which any bit of integer part of the selected coordinates of

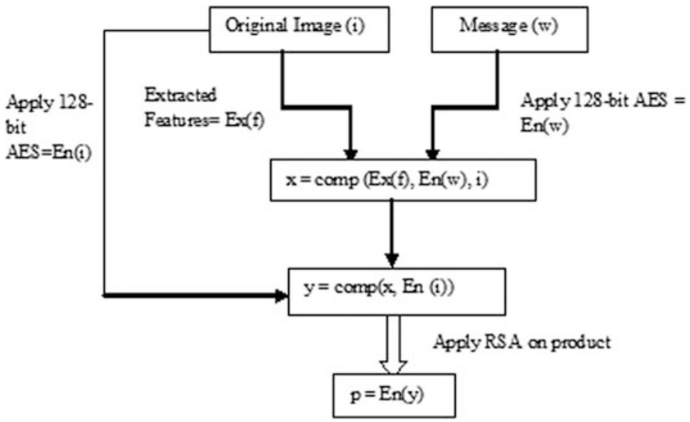

Fig. 1 Encryption at sender side

image is extracted and used [2]. The sequence of steps taken at sender and receiver side is shown as (Figs. 1, 2).

Encryption Algorithm (i,w)

```
Input: i = original image, w = original message
Step 1:
  1.1 Extract LSB from i using function Ex(f).
  1.2 Apply 128-bit AES on w by using encryption function, En(w).
Step 2: Apply composite function to embed encrypted message and extracted
features into image i, i.e.
        x = comp(Ex(f), En(w), i)
Step 3: Encrypt i using 128-bit AES encryption function, En(i).
Step 4: Apply composite function again on data structures obtained from
step 2 and 3.
       y = comp(x, En(i))
Step5: Obtain final message product p being ready to transmit over insecure
channel by encrypting y using RSA encryption function, i.e. p = En(y)
```

5.1 Explanation

The whole process of encryption and decryption passes through three stages of encryption at sender side and decryption at receiver side. At first stage, message which is to be sent by embedding it into an original image is encrypted using 128-bit AES algorithm in parallel extraction of least significant bits from original

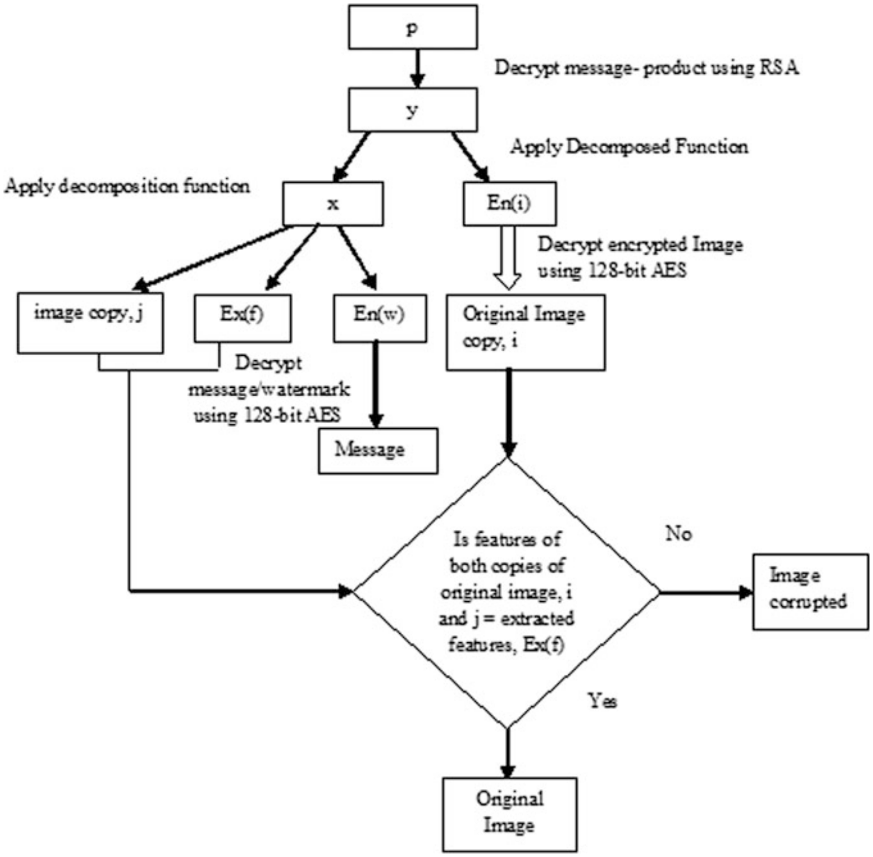
p
Decrypt message- product using RSA
y
Apply Decomposed Function
Apply decomposition function
x
En(i)
Decrypt encrypted Image using 128-bit AES
image copy, j
Ex(f)
En(w)
Original Image copy, i
Decrypt message/watermark using 128-bit AES
Message
Is features of both copies of original image, i and j = extracted features, Ex(f)
No
Image corrupted
Yes
Original Image

Fig. 2 Decryption at receiver side

image coordinates so that composition function can be applied over them. Extracting LSB helps in storing information of the image like checksum, compressed bits, etc.; here, in the proposed system checksum is stored in LSB for verification at other end. If at the other end the value of checksum founds to be different, then it can be identified that image has been tampered. After applying the composition function, comp(Ex(*f*), En(*w*), *i*), we get composite image, *x*, which is a combination of encrypted message, En(*w*), and extracted features (first bit of coordinates), Ex(*f*). In the second stage, complete product, *y*, gets obtained by combining the composite image with an encrypted original image being obtained after using 128-bit AES algorithm over it. Now, this envelope will hold composite image, *x*, and encrypted image, En(*i*). At last, the complete product will again get encrypted; using RSA algorithm, public key will be transmitted over the network for the user(s).

Decryption Algorithm (p)

```
Input: p = Encrypted message product received from insecure communication
channel
Step 1: Decrypt p using RSA algorithm, y = De(p).
Step 2: Apply decomposed function, decomp on the decrypted message product
y, obtained from step 1.
            (x, En(i)) = decomp(y)
Step 3: Obtain image i by decrypting En(i) using 128-bit AES algorithm and
in parallel apply decomposed function on x to get encrypted message En
(w),
extracted features Ex(f) and another copy of original image say j.
 i = De(En(i))
(j, En(w), Ex(f)) = decomp(x)
Step 4: Decrypt message using 128-bit AES algorithm, i.e. w = De(En(w)).
Step 5: Compare both copies of image stored in data structure i and j
respectively with extracted features Ex(f) and check whether the image has
been tampered or in the original form.
  If LSB(i) = LSB(j) = Ex(f)
   Then
          “Image not tampered”
   Else
          “Image tampered”
```

5.2 Explanation

Similarly, at receiver end decryption process will be applied. First, the complete encrypted product, *p*, gets decrypted using RSA and then decompose into two parts *x* and En(*i*) (selected bits of the coordinates). Now, *x* will be decomposed by applying decomposition function on *x*, and hence we will get Ex(*f*), En(*w*), and copy of original image, *j*. Next, both encrypted message, En(*w*), and encrypted image, En(*i*), get decrypted using 128-bit AES algorithm. This decrypted copy is an another copy of the same original image, say *i*. Now by comparing the extracted feature (bits) with features of both of these copies of original image, *i* and *j*, we can easily judge whether the image being received is distorted or not.

6 Conclusion

Under this research paper, we proposed a system that provides security at three levels. If an intruder is somehow able to decrypt the data at any of these levels, then it will be very difficult to decrypt at all levels. We have provided the security mix of symmetric and asymmetric cryptography that increases the security of the system. The proposed system can be used in the applications where sensitive information is needed to be transferred.

7 Future Scope

In this research paper, we have just proposed a system that could be implemented for providing efficient security to the organizations, businesses, military, medical, etc. Although the system provides security at three stages using symmetric as well as asymmetric algorithm, however, the use of other asymmetric algorithm for final stage could make system more secure, efficient, and accountable. Since the proposed system does not support any experimental data set, hence, it needs to be implemented for its actual result with strong mathematical foundation, comparing it with other algorithms on the basis of parameters like performance, efficiency, and complexity.

References

1. Abbas TA, Jawad MJ (2013) Proposed an intelligent watermarking in GIS environment. J Earth Sci Res (JESR) 1(1):1–5
2. Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2007) Digital watermarking and steganography (2nd edn). USA: Morgan Kaufmann
3. Dakroury Y, El-ghafar IA, Tammam A (2010) Protecting GIS data using cryptography and digital watermarking. Int J Comput Sci Netw Secur (IJCSNS) 10(1):75–84
4. Wayner P (2008) Disappearing cryptography: information hiding: steganography & watermarking (3rd edn). USA: Morgan Kaufmann
5. White Paper (2014) GIS platform for national security. http://www.esri.com/library/whitepapers/pdfs/gis-platform-for-national-security.pdf
6. Wolthusen S (1998) On the limitations of digital watermarks: a cautionary note. Available at http://www.wolthusen.com/publications/SCI1998.pdf
7. Satyanarayana P, Yogendran S, Military applications of GIS. http://geospatialworld.net/Paper/Technology/ArticleView.aspx?aid=908