Annals of the University of Craiova, Math. Comp. Sci. Ser.
Volume 35, 2008, Pages 97–102
ISSN: 1223-6934

3D Steganography Models

Mihai Dupac and Nicolae Constantinescu

Abstract. In this paper the way to communicate over a network by two parties, how to agree on a symmetrical encryption and how a cryptographic key is created will be discussed. The paper review a new proposed method, starting from sharing a common information. The difference reside in the way the information is combined inside the original image. Starting from the classic form of hiding information in a particular and characteristic image, a specific message will be hidden in a 3D natural environment scene. The 3D scene is generated using a grayscale height map (for terrain generation) and a Lindenmayer system (for the generation of plants). It is intended to include the common information inside a layer part of a multilayer image.

2000 Mathematics Subject Classification. 11T71; 68U05; 94A08.
Key words and phrases. Steganography, public key cryptography, 3D image generation, L-systems.

1. Introduction

Starting to define the steganography is likely to define the history of the cryptography. The main application in steganography is to convert the communication and digital multimedia data, such as movies and static pictures which are often used as host media, for a short most valuable information. The main idea is to include the information into a multilayer image, that can be defined as a 3D image. This kind of technique can be the start of an symmetric encryption system based on a common agreed session key ([3]). The information is split into streams and each stream has a coding that will be inserted into a selected layer in a multilayer image.

Modeling of realistic 3D image is a challenging problem in computer graphics. Realistic 3D images (such as 3D terrain models covered with vegetation) have a wide range of potential applications, including visualization and design for research and educational purposes, computer animation and games, and more than that, information encryption in the 3D scenes.

In the recent years, natural environment modeling (terrain covered with vegetation) has received considerable attention. Reeves and Blau [10] organized ecosystems by specifying the terrain map, the vegetation creation (individual plants modeling) and placement, and the model rendering (to incorporate light in the environment). Geometrical structures with defined branches length and angle have been used to create vegetation [2].

A different strategy for modeling natural environment, with the terrain and the vegetation modeled quadric surfaces, was proposed in [9]. A very accurate natural environment 3D image rendering and representation was presented in [8].

A different approach for plants modeling and scenes, based on rules and specification of plants topology, has been used in [15, 16] and [4].

Received: 23 November 2008.

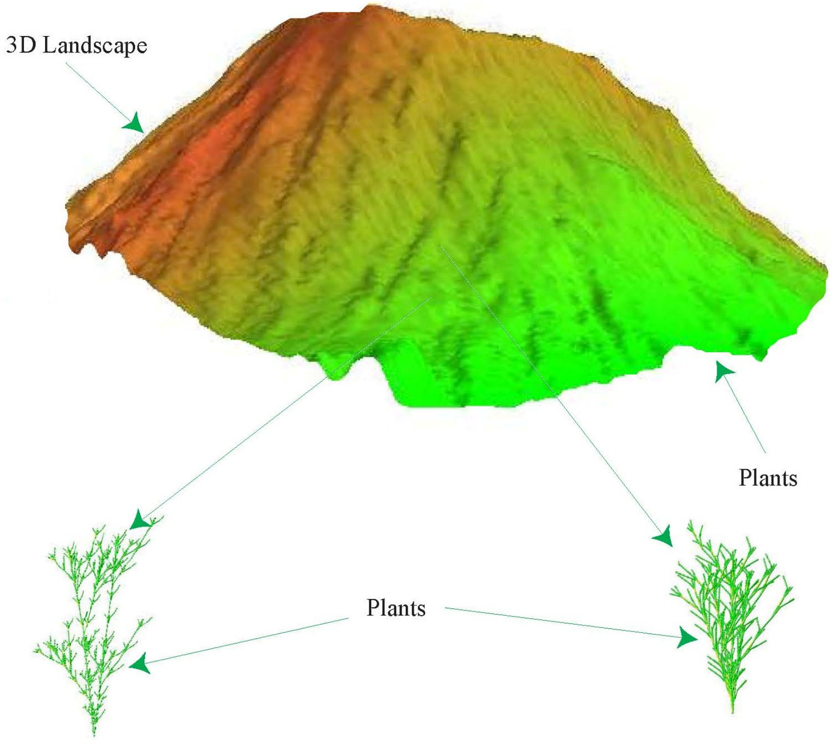

Figure 1. 3D terrain map covered with vegetation based on a L-system individual plants modeling and placement

In this paper a key pair which use a 3D model like a seed have been generated. The used 3D image model environment assure that the complexity of the nonlinear attack include those key pairs in a stable model. For the modeling of the 3D image (terrain and/or vegetation scenes) for encryption purpose a grayscale height map and a L-system, i.e., Lindenmayer system, (used in biology for the modeling and simulation of plants growth processes [13, 14, 17]), have been used. As future work, it is intend to include the common information inside a layer part of a multilayer image.

2. 3D Image Generation - Terrain and Plants Modeling

In this section 3D terrain surface and plants generation are presented. The 3D terrain surface is modeled using an Digital Elevation Model (DEM), i.e., a sampled array of elevations for a number of ground positions. Two standard techniques may be used to define a DEM, the use of numerical height maps, or a grayscale image height map. A numerical height map is a two dimensional array of numerical values that indicates the elevation of the terrains surface. In a grayscale image height maps the brightness of each image pixel represents the height of the terrain at that coordinate. The second techniques have been used to generated the terrain as shown in Fig. 1.

Parallel rewriting systems commonly referred to as L-systems have been used for three-dimensional plants modeling as shown Fig. 1. The 3D terrain scene, generated using grayscale image height maps technique, was covered lately with plants (the green area in Fig. 1 represents vegetation).

Classically, an L-system is specified by three components: the alphabet (a set of labels edge), the axiom (an axial tree with labels from the alphabet), a production rules set. An L-system is deterministic if for any alphabet and any context there is only one production rule, otherwise the L-system is nondeterministic. By applying the rules a sequence of words may is generated.

To translate the expressions into 3D structures (3D plants) a geometrical interpretation of the strings, so-called turtle geometry [1] is used. The turtle is like a virtual drawing tool, that change its position and orientation in the 3D space, while drawing graphical elements (plant stalks, plant leafs, plant flowers). A Cartesian coordinate system is usually used to represents the turtle geometry, i.e., position and orientation, and other attribute values such as width and color.

For the present case the turtle initial position is given by the coordinate of the terrain height, and the turtle orientation is given by a 3D orthogonal vectorial system. Two L-systems three-dimensional plants modeling created using the previously described technique are shown in Fig. 1.

3. Encryption Scheme

3.1. The Confidentiality. In order to ensure the communication's confidentiality, the following three requirements must be resolved:

(1) The generation and distribution of the master key.

(2) The agreement of a protocol which would generate a session key, which would be used by the communicative parties, for the current message exchange session.

(3) The information encryption algorithm for the key which both parties have agreed on.

This system is useful in the case when a symmetrical encryption key of the messages is used, and an agreement on a ciphering key (the session key), based on public keys encryption, is made. The initial idea which led to the development of the identity based system, belongs to Shamir [11], who wanted to create a method of assuring e-mail confidentiality. Let there be Alice and Bob, the two parties who want to communicate. Both have an e-mail address. When Alice wants to send a message to Bob, she will be accessing a Server which stores Bob's public key, and she will use this key to encrypt information. The Server will store both parties private and public keys. A key request will take place when the Server receives a message which contains the e-mail address of the one who's public key is asked for. Shamir [11] simplified the system by introducing a function, χ, which generates a public key based on a random string (e-mail address). In this way, Alice will not be requesting the key from the Server anymore, instead she will use the key which was generated by the χ function. The usefulness of the system resides in the fact that one can encrypt and send messages to somebody on the network even if the password Server is unavailable, and it also eliminates the need to gain access to the password Server for the dialog's counterpart. A series of algorithms and protocols which are based on this system have been developed [7, 12], but not all of them can be used in real life due to the burden that some of these algorithms and protocols impose on modern computing systems.

3.2. The description of identity based confidentiality system. In [5], the authors elaborated an identity based system. This system is composed by the following parts:

(1) *The system's setup.*
To each dialogging party the password Server assigns a control key, called ID. This key is used by the Password Server to communicate with it's users. The Password Server will be called PKG (*Public Key Generator*)from now on.
(2) *Encryption.*
A participant, called A, who wants to communicate with another (called B), will encrypt the message, which will be send, with a public key, called p_k, obtained from the morphing, through function χ, of a string s which contains B's identifier (which can also be B's address).
(3) *Decryption.*
A system's user who will receive such messages, will access the PKG and, based on his ID, will obtain the private key with which he can decrypt the message.

3.3. Blind Signature Stream Transmission. The way of secured transmission consists in adding the information into each selected layer, starting from Shaos Improved User Efficient Blind Signature Scheme, and by split the streams into encoded information, in four phases:

The Initialization Phase
The signer computes $n = pq$, where p, q are two large primes (analogus with [6]), and $p \equiv q \equiv 3(\mod 4)$. Furthermore, let H be a one-way hash function. The signer keeps p and q secret, and publishes n and H.

The Requesting Phase
To obtain a signature of the message m, the requester randomly chooses two integers u and b, such that

$$\alpha = b^2 H(m)(u^2 + 1) \bmod n. \tag{1}$$

Then the requester delivers α to the signer.

The Signing Phase
While receiving α, the signer randomly chooses an integer x. Because the signer knows the factors p and q of n, and $\alpha(x^2 + 1) \bmod n$ is a QR in $\mathbb{Z}_n^*$, therefore, the signer has the ability to derive t from

$$t^{-2} = \alpha(x^2 + 1) \bmod n. \tag{2}$$

Then, the signer delivers the pair (t, x) to the requester (see [6]).

The Extraction Phase After receiving (t, x), the requester computes

$$c = (ux - 1)(x + u)^{-1} \bmod n, \tag{3}$$

and

$$s = bt(x + u) \bmod n. \tag{4}$$

The pair (c, s) is a signature of m. To verify the validity of (c, s) of m, the verifier checks whether or not the following equation holds,

$$H(m)s^2(c^2 + 1) = 1 \bmod p. \tag{5}$$

In the following, we prove that equation 5 always holds while the signature (c, s) is correct. According to equation 2, we get

$$t^2\alpha(x^2 + 1) = t2t - 2 = 1 \bmod n. \tag{6}$$

Hence, we have

$$\begin{aligned}
&H(m)s^2(c^2+1)\\
&=(\tfrac{\alpha}{b^2(u^2+1)})(bt(x+u))^2((\tfrac{ux-1}{x+u})^2+1)\\
&=(\alpha b^2(u^2+1))(bt)^2((ux-1)2+(x+u)2)\\
&=(\alpha b^2(u^2+1))(bt)^2(x^2+1)(u^2+1)\\
&=t^2\alpha(x^2+1)=1(\mod n).
\end{aligned}$$

3.4. Insertion Scheme. Starting from the selected layers created by statistically analyze of the contained information, the amount of a certain stream encoded information is added to the layer, using the next common scheme:
Insertion-LSB
Substitution
Generation

Definition 3.1. *(Secret key steganography) The quintuple $\Psi =< C, M, K, D_K, E_K >$, where C is the set of possible covers, M the set of secret messages with $|C| \geq |M|$, K the set of secret keys, $E_K : C \times M \times K \to C$ and $D_K : C \times K \to M$ with the property that $D_K(E_K(c, m, k), k) = m$ for all $m \in M, c \in C$ and $k \in K$, is called a secret key selenographic system.*

The previous definition show how to add to a mathematical model a specific information about a system used like a carrier.

Each of previous technics can add a short information into a most complete part of a image by inserting an encoded stream into Blind Signature Scheme of a previous layer stream. Hereby, in a layer, a image is composed of dots called pixels. Putting together all these pixels, a stream is formed. The stream can be split into substreams with more or less statistically representation. Selecting the most representative parts, the *representative streams* from the each layer is formed. Selecting an encoded scheme and starting from the representation of a color, an encoded stream which don't change the statistic for the layer is created. If the statistic is in a specific range specified in the start of the protocol, the next layer of the image like a *feasible layer* is chosen in order to hide information. A secret key is created, to ensure the coding function for the next layer (according with 3.1).

4. Conclusions

In this paper a way to communicate over a user's channel, that can bring together a common information, and using a multilayer image like a host, is described. The way to generate the particular images which can support this type of information it was also presented. This kind of system problems are related to the length of the messages exchanged by the participants, based on the same string structure. In practice a set of preliminary information is used to generate the particular structure, that can include the necessary uncorrupted information. The proposed model limits the number of valid messages that can be transmitted. Also, the number of the encoded strings by an amplification factor, takes into account the frequency of the communication between each secured participant. Starting by analyzing the presented model, there is a case that include an asymmetric key encryption, which conclude the increase power of the encryption scheme.

4.1. Future Work. Based on the previous presented scheme a common way to generate images and hide information, as a integrated part of a system that may secure transmission between a set of users, will be proposed.

Acknowledgments. One of the authors has been supported by CNCSIS Grant 55/2008.

References

[1] H. Abelson and A. A. diSessa. Turtle Geometry. M.I.T. Press, Cambridge, 1982.

[2] Aono, M., and Kunii, T. L. Botanical tree image generation. IEEE Computer Graphics and Applications 4, 5 (1984), 10-34.

[3] N. Constantinescu, The agreement of the common key, *The Annals of the University of Craiova - Mathematics and Computer Science series*, Vol. XXX, 2004

[4] Beyer, T., and Friedell, M. Generative scene modelling. Proceedingsof EUROGRAPHICS '87 (1987), 151-158 and 57I.

[5] N. Constantinescu, G. Stephanides, Identification of parts in identity-based encryption, *Research Notes in Data Security, Wessex Institute of Technology*, UK, developed with University of Bergen, Norway, ISBN 1-85312-713-2, 2004

[6] N. Constantinescu, George Stephanides, Secure Key-Exchange, *Recent Advances in Communications and Computer Science* , Vol. 7,pp. 162-166, WSEAS Press, Greece, 2003

[7] A. Miyaji, M. Nakabayashi, S. Takano, New explicit condition of elliptic curve trace for FR-reduction, *IEICE Trans. Fundamentals*, Vol. E84 A, No. 5, May 2001

[8] O. Deussen, P. Hanrahan, B. Lintermann, R. Mech, M. Pharr, P. Prusinkiewicz, Realistic modeling and rendering of plant ecosystems, Proceedings of SIGGRAPH 98 (Orlando, Florida, July19-24, 1998). In Computer Graphics Proceedings, Annual Conference Series, 1998, ACM SIGGRAPH, pp. 275-286.

[9] N. Max. Hierarchical rendering of trees from precomputed multi-layer Z-buffers. In X. Pueyo and P. Schroder, editors, Rendering Techniques 96, pages 165174 and 288. Springer Wien, 1996.

[10] Reeves, W. T., and Blau, R. Approximate and probabilistic algorithms for shading and rendering structured particle systems. Proceedings of SIGGRAPH '85 (San Francisco, CA, July 22-26, 1985). In Computer Graphics 19, 3 (1985), 313-322.

[11] A. Shamir, Identity-based cryptosystems and signature schemes, *Advances in Cryptology*, LNCS, Vol 196, Springer-Verlag, pp. 47-53, 1984

[12] H. Tanaka, A realization scheme for identity-based cryptosystem, *Advances in Cryptology*, LNCS, Vol 293, Springer-Verlag, pp. 341-349, 1987

[13] Jacob, C. 1994, Genetic L-System Programming. Parallel Problem Solving from Nature - PPSN III, Lecture Notes in Computer Science 866, Berlin, Springer.

[14] Lindenmayer, A. 1968, Mathematical models for cellular interaction in development, Parts I and II, Journal of Theoretical Biology, 18:280-315.18:280-299 and 300-315, 1968.

[15] P Prusinkiewicz, A. Lindenmayer, and J. Hanan t. Developmental Models of Herbaceous Plants for Computer Imagery Purposes, Computer Graphics, Volume 22, Number 4, August 1988

[16] P Prusinkiewicz. Applications of l-systems to computer imagery. In H Ehrig, M Nagl, A Rosenfeld, and G Rozenberg, editors, Graph grammars and their applications to computer science; Third international workshop. Springer-Verlag, 1987.

[17] P Prusinkiewicz and A Lindenmayer. The Algorithmic Beauty of Plants. Springer-Verlag, New York, 1990.

(Mihai Dupac, Nicolae Constantinescu) Department of Mathematics, University of Craiova, Al.I. Cuza Street, No. 13, Craiova RO-200585, Romania, Tel. & Fax: 40-251412673
E-mail address: `mihaidupac, nikyc@central.ucv.ro`