# Steganography with Public-Key Cryptography for Videoconference

**Fábio Borges** **Renato Portugal** **Jauvane Oliveira**
National Laboratory of Scientific Computing - LNCC
25651-075, Petrópolis, RJ
E-mail: borges@lncc.br portugal@lncc.br jauvane@lncc.br

## Abstract

In this work, we show a model for a case where extreme security is needed. In such case steganocryptography (steganography and cryptography) is used. In this model we use Diffie-Hellman, RSA and cryptography with irrational numbers. We use also steganography in DCT coefficients to send a message through the frames.

## 1 Introduction

Steganography is the art of hiding a message in a given media, whereas cryptography is the art of encoding a message so that no one can understand it. They are two different principles. In the former one an eavesdropper could read the message if he or she knows where it is hidden, whereas in the latter one, he or she knows about a given message, but it can't be understood. A natural question would be: If the current cryptography in not broken, why would it be necessary to use steganography?

Most of the public-key cryptosystems, in practice, do not need a trusted arbitrator, for example: cryptographic personal home pages or e-mails.

However, the banks do need a trusted arbitrator because an outlaw could do "spoofing" [24, 21], namely, he or she could prepare a machine to mimic the bank and, therefore, steal the client.

In this case, extreme security, there are lots of reasons to use steganography, from which we mention three below:

- The enemy could interrupt the message, which may cause worse implications if we don't know that such message has been interrupted. Such case is less likely to happen when steganography is used.
- There is the Shor's quantum algorithm [23, 16] that can factor huge numbers quickly $O(n^3)$, in which $n$ means the number of the integer digits. As the majority of the public-key cryptosystems are based on commutative groups, they could be broken when the technology provides an increase in the qubit numbers of a Quantum Computer. Perhaps it is not as hard as it seems [3]. In short, nobody knows whom or when a Quantum Computer of considerable size could be built.
- Except for *perfect secrecy* [22], namely One-Time-Pad, the inviolability of any cryptosystems has never been proved. Therefore someone might find a way to break the cryptosystem, just like an algorithm that determines if a number is prime in polynomial time has been sought for centuries and suddenly found [1, 15].

Now, let us remember that steganography does not work only with computer files, but we can embed data in protocols, namely TCP/IP[2], or we can hide data in the DNA [7, 6].

In the section 2 and 3, we will improve the idea of embed data in videoconference [26] increased the protection of the message.

## 2 Steganography

Steganography using public-key cryptography cannot use a static media, like an image, but it requires a data stream, like a dialog.

Furthermore, we need a huge amount of data to embed the message. This is the reason why

we chose a videoconference. A good steganography should not be based on the amount of available media, but rather on the difficulty of finding it in the media [17]. For the system to be secure we must bear in mind Shannon's maxim: "the enemy knows the system".

Notice that we should be working with the media properties to embed a message in such media.

### 2.1 Videoconference

Basically we have the option to use the sound or the video, for steganography. In this work, we chose the video.

We chose the ITU-T H263 Recommendation [10] - video codec protocol.

An H263 video stream contains I-frame, P-frame and B-frame. In this work we focus on steganography embedded in I-frames due to the fact that they do not contain motion estimation and compensation. See [8] for more details.

We could choose H264 but it has also matrix 4x4 and 16x16, moreover it is wavelet-based [18] when H263 works only with 8x8 matrices and is DCT-based [20].

### 2.2 Hiding

In a bit map if we change the Least Significant Bit (LSB) of each pixel, we get vulnerable to visual attacks. However, in a JPEG[1] [11] picture (which is similar to an I-frame) if we change the LSB in the frequency domain then the visual attack is unsuccessful in the JPEG image [17]. For simplicity, we transform the stream video in a sequence of JPEG. The JPEG uses the Discrete Cosine Transform (DCT) that is given by

$$F[m,n] = \frac{C(m)}{2}\frac{C(n)}{2}\sum_{x=0}^{7}\sum_{y=0}^{7} P[x,y]\cos\alpha\cos\beta, \tag{1}$$

where $m$ and $n$ vary from 0 through 7, $P[x,y]$ is the pixel matrix,

$$\alpha = \frac{(2x+1)m\pi}{16},$$

$$\beta = \frac{(2y+1)n\pi}{16}$$

and

$$C(k) = \begin{cases} \frac{1}{\sqrt{2}} \text{ for } k = 0, \\ 1 \text{ for all other values of } k. \end{cases}$$

After having applied the DCT (1) in each 8x8 pixel matrix, we have the DC coefficient, where m+n=0, which provides the average color of the block, as well as the AC coefficients, which are all other coefficients.

The quantization (2)

$$F'[m,n] = \frac{F[m,n]}{Q[m,n]} \tag{2}$$

is then applied. It is possible to control the compression rate, having some loss of image information, through quantization adjustments.

The last stage of JPEG compression is a lossless entropy encoding.

The interesting place to embed information is between the quantization and the entropy encoding. See figure 1.

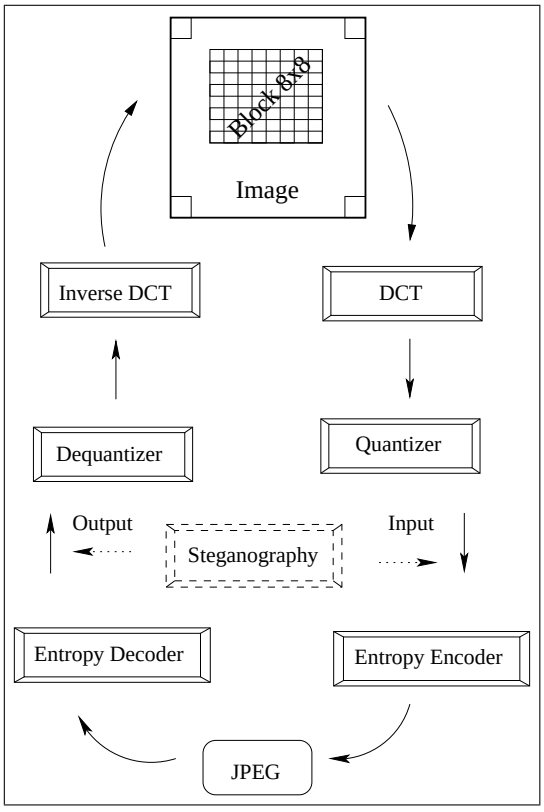


Figure 1: *Steganographic scheme in JPEG.*

If the AC coefficients, different from zero and one, have the LSB changed in a sequential way, a statistical attack can estimate, with good precision, the length of the message [17, 25].

[1] JPEG - Joint Photographic Experts Group.

The statistical attack is efficient because the bit pairs that differ only from the last digit tend to have the same frequency, once the transmitted message is encoded or compacted.
However, if the $F'$ matrices are randomly chosen, the difficulty in determining the presence of a steganographed message increases considerably.
In general, the difficulty in detecting $D$ is inversely proportional to the length of the message $L_{me}$ and directly proportional to length of the media $L_{mi}$ and to how spread the message $S$ is. In summary

$$D = \frac{SL_{mi}}{L_{me}}. \tag{3}$$

As our goal is to maximize $D$, we must spread the message in the media.
There is no control over the size of message, but the equation (3) justifies the media choice, whose only size limitation is the time.
Besides choosing the matrices $F'$ randomly, we can also change a small number of elements this way.

Now consider the pixel matrix $P$ given by

$$P = \begin{bmatrix} 0 & 0 & 0 & 200 & 200 & 0 & 0 & 0 \\ 0 & 0 & 200 & 200 & 200 & 200 & 0 & 0 \\ 0 & 200 & 200 & 200 & 200 & 200 & 200 & 0 \\ 200 & 200 & 200 & 200 & 200 & 200 & 200 & 200 \\ 200 & 200 & 200 & 200 & 200 & 200 & 200 & 200 \\ 0 & 200 & 200 & 200 & 200 & 200 & 200 & 0 \\ 0 & 0 & 200 & 200 & 200 & 200 & 0 & 0 \\ 0 & 0 & 0 & 200 & 200 & 0 & 0 & 0 \end{bmatrix}$$

and the quantization matrix $Q$ given by

$$Q = \begin{bmatrix} 6 & 11 & 16 & 21 & 26 & 31 & 36 & 41 \\ 11 & 16 & 21 & 26 & 31 & 36 & 41 & 46 \\ 16 & 21 & 26 & 31 & 36 & 41 & 46 & 51 \\ 21 & 26 & 31 & 36 & 41 & 46 & 51 & 56 \\ 26 & 31 & 36 & 41 & 46 & 51 & 56 & 61 \\ 31 & 36 & 41 & 46 & 51 & 56 & 61 & 66 \\ 36 & 41 & 46 & 51 & 56 & 61 & 66 & 71 \\ 41 & 46 & 51 & 56 & 61 & 66 & 71 & 76 \end{bmatrix}.$$

In sequence, we applied the DCT to $P$ and the quantization to the result. Then, we applied the dequantization and the inverse of DCT. We have some matrices and except for the matrix $A$, the others will suffer steganography.

So, using the Euclidean distance as metric, we can evaluate how much the matrix changes.

Consider the matrices:

- $A$ that has not suffered steganography,
- $B$ that has changed in every second LSB of coefficients AC, whose modulus is greater than two,
- $C$ that has changed only the second LSB of $F'[0, 2]$,
- $D$ that has changed the LSB of AC, whose modulus is greater than one.

Considering the matrices as vectors and calculating the Euclidian distance, we have:

- $|P - A| = 35.60898762$
- $|P - B| = 200.2698180$
- $|P - C| = 48.98979486$
- $|P - D| = 106.5833008$

As we can see, in this case, changing the second LSB of just one AC coefficient is more interesting than changing the first of all AC coefficients, whose modulus is greater than one, as currently done.

In the figure 2 we can see a graphic representation of the matrix $A$, that has not changed, compare with the figure 3 from the matrix $B$ and the figure 5 from the matrix $D$, that has steganography in many coefficients.

Now compare the figure 2 with the figure 4, that has changed only the second LSB of $F'[0, 2]$. We can see that the figure 2 is similar to the figure 4 when the figures 3 and 5 are very different. Therefore the Euclidean distance is a good metric to see the distortions in these images.

Based on the Euclidean distance and figures from matrices we conclude that the technical used in matrix $C$ is better. Thus, we propose in this model to change one bit per matrix, which can be the first or the second LSB. That prevents the mentioned above statistical attack from happening. A pseudo-random number gives the matrix chosen as well as the position, which is to be changed. This number is arranged with the RSA [19]. The RSA keys are exchanged from fixed positions of bits in the image, in a way that did not alter the image.

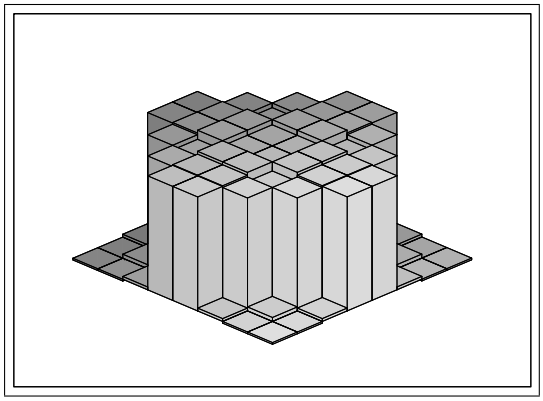

Figure 2: *Matrix A without steganography.*

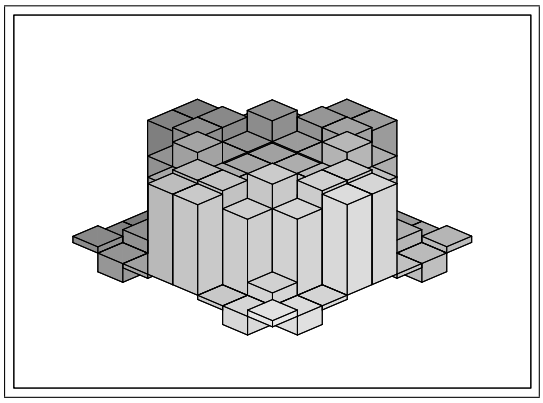

Figure 3: *Matrix B with aggressive settings.*

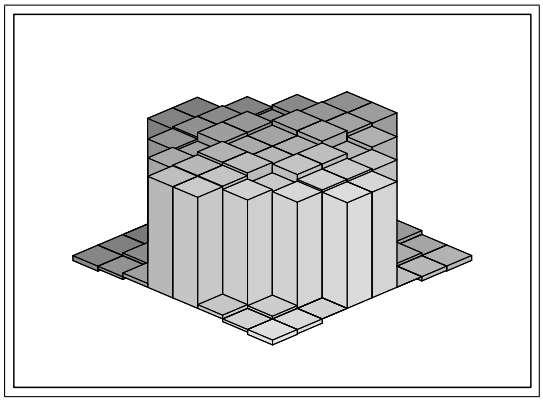

Figure 4: *Matrix C no aggressive settings.*

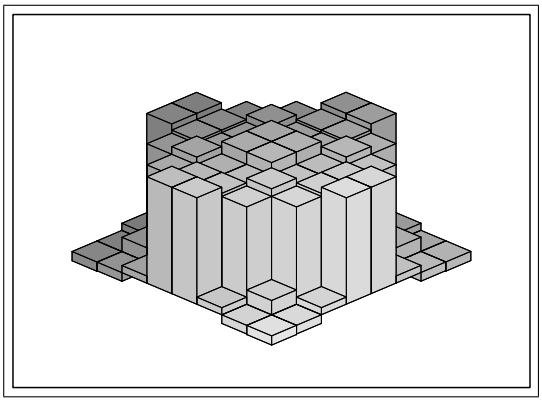

Figure 5: *Matrix D with aggressive settings.*

We can implement another public key cryptosystem when the key should be shorter, namely Elliptic Curve Cryptosystem (ECC) [14, 9].

# 3 Cryptography

In our implementation we are using RSA public-key cryptosystem and the Diffie-Hellman key exchange protocol [12, 13, 5].

The RSA cryptosystem is based on good choice of two prime numbers $p$ and $q$, and encipher in blocks, the greater the prime numbers, the greater the blocks.

Consider that Alice wants to receive encoded information. She must calculate

$$\varphi = \varphi(pq) = (p-1)(q-1)$$

and choose $a$ so that $\gcd(a, \varphi) = 1$, being able, therefore, to determine some $b$ so that

$$ab \equiv 1 \bmod \varphi.$$

Ensuring that

$$x^{ab} \equiv x \bmod pq \quad \forall x \in \mathbb{Z}.$$

Then Alice can hide $a$ and disclose $b$ as a public key.

Imagine that Bob wants to send messages to Alice, than he must know $b$. However, if $b$ was transmitted by an insecure line of communication, Bob might be using $b_1$, instead of $b$, since an eavesdropper might replace $b$ by $b_1$. In order that only the eavesdropper who knows $a_1$ can read the message.

Alice and Bob could use the Diffie-Hellman method to transmit the key secretly. In this

method all the numbers are in $\mathbb{Z}_{pq}$. Alice chooses $k$ with $gcd(k, pq) = 1$ and sends the values of $k$ and $pq$. Then, Alice chooses a $r$, computes $k^r$ and sends the result to Bob while keeping $r$ secret. At the same moment Bob chooses $s$, computes $k^s$ and sends the result to Alice while keeping $s$ secret.

So, both form the candidate exponent

$$a = (k^r)^s = (k^s)^r.$$

To verify if $a$ is a valid RSA exponent, Alice computes $gcd(a, \varphi) = 1$. If $a$ is not valid they repeat the process.

However, this message does not guarantee that Alice is talking to Bob. An intruder could be changing the key instead of Bob. Someone should guarantee that only $b$ is the true Alice's key or that Bob is talking to Alice. For this reason, the banks use a trusted arbitrator.

In this model, the intervention of a trusted arbitrator is not necessary, because Alice and Bob are in a videoconference.

Due to the computational high cost of the RSA along with the media processing, we need a symmetric cryptography. That is why Diffie-Hellman is only used to arrange a pseudo-random number to be used in the steganography and a generator of an irrational number, namely square root of a prime number [4], to be used in the cryptography.

Then, with the irrational number expansion we encipher same as the One-Time-Pad. If the message is sufficiently big for the expansion to consume much processing, Alice and Bob may arrange new irrational number through the RSA. Remember that there are more irrational than rational numbers.

A natural question is: How do we start the communication before Diffie-Hellman key agreement? We use a fixed sequence in the videoconference to find a prime number and so a pseudorandom sequence to send the ciphered and embed message. As the sequence of bits is fixed, it would be quiet suspicious if it formed a prime number, thus we take the less prime greater than the number formed by the sequence.

In summa, our protocol has five stage of protection, it uses:

1. the position of the sequence of bits previously agreement to establish communication in a videoconference,
2. steganography more secure,
3. Diffie-Hellman key agreement,
4. RSA to exchange an irrational number generator,
5. strong cryptography based on irrational numbers.

As result we implemented a prototype that uses a strong cryptography and a steganography with less distortion in the I-frames (JPEG) to transfer data through videoconference.

# 4 Conclusion

We have introduced a model for steganocryptography. We believe that such model brings an extra-layer of security for applications which require extreme security. Our model is robust against most common attacks, like statistical attacks. Future work will be devoted to ECC and embed the cryptography into fewer coefficients but more bits in the same coefficient.

# References


[1] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Ann. of Math. (2)*, 160(2):781–793, 2004.

[2] K. Ahsan and D. Kundur. Practical data hiding in tcp/ip, 2002.

[3] M. P. Almeida, F. de Melo, M. Hor-Meyll, A. Salles, S. P. Walborn, S. P. H. Ribeiro, and L. Davidovich. Environment-induced sudden death of entanglement. *Science*, 316(5824):579–582, April 2007.

[4] F. Borges, R. Portugal, and J. C. Oliveira. Criptografia com números irracionais. *Anais do Congresso de Matemática e suas Aplicações*, 1:1–2, 2006.

[5] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976.

[6] U. Feldkamp, W. Banzhaf, and H. Rauhe. A DNA sequence compiler. In *Proceedings 6th DIMACS Workshop on DNA Based Computers, held at the University of Leiden, Leiden, The Netherlands, 13 - 17 June 2000*, page 253, 2000.

[7] A. Gehani, T. H. LaBean, and J. H. Reif. DNA-based cryptography. In E. Winfree and D. K. Gifford, editors, *Proceedings 5th DIMACS Workshop on DNA Based Computers, held at the Massachusetts Institute of Technology, Cambridge, MA, USA June 14 - June 15, 1999*, pages 233–249. American Mathematical Society, 1999.

[8] F. Halsall. *Multimedia Communication: Applications, Networks, Protocols*. Addison-Wesley, 2001.

[9] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to elliptic curve cryptography*. Springer Professional Computing. Springer-Verlag, New York, 2004.

[10] I. T. U. ITU-T. Itu-t recomendation h.263, 1998.

[11] I. T. U. ITU-T. Itu-t recomendation t.86, 1998.

[12] R. E. Klima, N. Sigmon, and E. Stitzinger. *Applications of abstract algebra with Maple*. CRC Press, Boca Raton, FL, 2000.

[13] N. Koblitz. *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato.

[14] N. Koblitz and A. J. Menezes. A survey of public-key cryptosystems. *SIAM Rev.*, 46(4):599–634 (electronic), 2004.

[15] R. A. Mollin. A brief history of factoring and primality testing b. c. (before computers). *Mathematics Magazine*, 75(1):18–29, feb 2002.

[16] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[17] N. Provos and P. Honeyman. Hide and seek: An introduction to steganography. *IEEE Security and Privacy*, 1(3):32–44, 2003.

[18] I. E. G. Richardson. *H.264 and MPEG-4 Video Compression*. Wiley, 2004.

[19] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[20] K. Sayood. *Introduction to Data Compression*. Morgan Kaufmann, 2000.

[21] B. Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. Wiley, New York, 2nd edition, 1996.

[22] C. E. Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28:656–715, 1949.

[23] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[24] W. Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson Education, 2002.

[25] A. Westfeld and A. Pfitzmann. Attacks on steganographic systems. In *IH '99: Proceedings of the Third International Workshop on Information Hiding*, pages 61–76, London, UK, 2000. Springer-Verlag.

[26] A. Westfeld and G. Wolf. Steganography in a video conferencing system. *Lecture Notes in Computer Science*, 1525:32–47, 1998.