# A Note on "MPEG Video Encryption Algorithms"

Shujun Li and Bharat Bhargava

August 12, 2004

**Abstract**

This short article points out that the result given in the Appendix of [Multimedia Tools and Applications, 24, 57–79, 2004] is incorrect.

In the Appendix of [1], it was claimed that the DC coefficient of a $8 \times 8$ DCT transform can be uniquely derived from the sum of all other 63 AC coefficient. This short article points out this result is incorrect.

In [1], the $8 \times 8$ DCT transform of an input block $[I(x,y)]_{8\times 8}$ is defined as follows:

$$F(u,v) = \frac{C(u)C(v)}{8} \sum_{x=0}^{7} \sum_{y=0}^{7} I(x,y) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2y+1)v\pi}{16}, \tag{1}$$

where $C(0) = \frac{1}{\sqrt{2}}$ and $C(u) = C(v) = 1$ when $u, v = 1 \sim 7$. Note that the above equation is different from the standardized one given in [2] and used in MPEG-1/2 standards [3, 4], which is defined as follows:

$$F(u,v) = \frac{C(u)C(v)}{4} \sum_{x=0}^{7} \sum_{y=0}^{7} I(x,y) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2y+1)v\pi}{16}. \tag{2}$$

Since the former Eq. (1) is an unintentional mistake of Eq. (2), this paper will focuses only the latter definition.

The result given in [1] can be formally described as follows[1]:

$$\left( \sum_{u=0}^{7} \sum_{v=0}^{7} F(u,v) \right) - F(0,0) = F(0,0) \cdot (1+\alpha), \tag{3}$$

where $\alpha$ is claimed to be "a set of cosine function" (but no explicit form is given). The above equation means the DC coefficients, $F(0,0)$, can be uniquely derived from other 63 AC coefficients by being divided by a constant, $1+\alpha$. We will show that this result is incorrect.

To prove the incorrectness of this result, let us construct a new DCT block $[F'(u,v)]_{8\times 8}$ as follows: $F'(u,v) = F(u,v)$ except for $F'(0,0) \neq F(0,0)$. Then, do IDCT to get a new input block $[I'(x,y)]_{8\times 8}$ as follows:

$$\begin{aligned} I'(x,y) &= \frac{1}{4} \sum_{u=0}^{7} \sum_{v=0}^{7} C(u)C(v)F'(u,v) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2y+1)v\pi}{16} \\ &= \frac{1}{4} \sum_{u=0}^{7} \sum_{v=0}^{7} C(u)C(v)F(u,v) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2y+1)v\pi}{16} + \frac{1}{4} \cdot C(0)C(0)(F'(0,0) - F(0,0)) \\ &= I(x,y) + \frac{1}{8} \cdot (F'(0,0) - F(0,0)). \end{aligned}$$

Apparently, $\forall x, y$, $I'(x,y) \neq I(x,y)$, and the difference between them is proportional to the DC difference $(F'(0,0) - F(0,0))$, which coincides well with the physical meaning of the DC component in DCT transform. If Eq. (3) is true, then $F'(0,0) = F(0,0)$, which conflicts with the fact that $F'(0,0) \neq F(0,0)$. As a result, one can immediately deduce that Eq. (3) must be incorrect. In fact, it can be easily obtained that $\alpha$ is not a constant, but the variable ratio between $F(0,0)$ and the other 63 AC coefficients.

[1] Note that two subscripts $y$ in the Appendix of [1] should be $v$, which should be typos. Also, there are some other inadequacies, such as the wrong reduction of $\frac{C(u)C(v)}{8}$.

# References


[1] Bharat Bhargava, Changgui Shi, and Sheng-Yih Wang. MPEG video encryption algorithms. 24(1):57–79, 2004.

[2] IEEE Standard Board. IEEE standard specifications for the implementations of $8 \times 8$ inverse discrete cosine transform. IEEE Std. 1180-1990, 1990.

[3] ISO/IEC. Information technology – coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s – Part 2: Video. ISO/IEC 11172-2, 1993.

[4] ISO/IEC. Information technology – generic coding of moving pictures and associated audio information: Video. ISO/IEC 13818-2, 2000.