Криптозащита растровых изображений и видеосигналов на основе алгоритмов быстрого преобразования Фурье

УДК 004.056.55

Анатолий Белецкий, Денис Навроцкий, Дмитрий Конюший

Национальный авиационный университет, [1]abelnau@ukr.net, [2]g6336@yandex.ua, [3]dima.konushiy.95@mail.ru

Важную роль в теории и практике помехоустойчивого кодирования и криптографической защиты информации играют матрицы Адамара, впервые введенные в математических обиход в конце XIX-го столетия. В 60-х годах прошлого века было замечено, что эти матрицы могут быть использованы для построения кодов с большим расстоянием Хэмминга $d = N / 2$, где $N = 2^n$, $n = 1, 2, \ldots$, — порядок квадратной матрицы Адамара.

Число симметричных систем Уолша $L_W(n)$, заданное соотношением

$$L_W(n) = \prod_{i=1}^{n} (2^n - \mathrm{mod}(i, 2)), \quad (1)$$

резко возрастает, как это показано в табл. 1, при увеличении показателя n степени двойки, совместно определяющих порядок N матриц Уолша $\boldsymbol{W}$.

Таблица 1

Оценка числа симметричных систем Уолша

n	1	2	3	4	5	6	7	8
$L_W(n)$	1	4	28	446	13’888	888’832	112’881’664	28’897’705’984

Системы функций Уолша успешно применяются для построения алгоритмов БПФ, доставляя, согласно табл. 1, при двукратном 256-точечном преобразовании возможность выбора из более чем 2^{68} различных базисов. В таком случае противник, пытаясь взломать зашифрованное посредством БПФ в секретных базисах Уолша, например, растровое изображение или видеосигнал, вынужден при лобовой атаке затрачивать ресурсы, практически не достижимые на современном уровне развития вычислительной техники.

Криптографические приложения алгоритмов БПФ в базисах классических систем функций Уолша опираются на такие фундаментальные соотношения.

Утверждение 1. *Каждая система (матрица) Уолша двоично-степенного порядка* $N = 2^n$ *однозначно представима своей индикаторной матрицей* $\boldsymbol{J}_W$ $n-$*го порядка.*

Теорема. *Индикаторными матрицами* (*ИМ*)*, систем функций Уолша* $\boldsymbol{W}$ *двоично-степенного порядка* $N = 2^n$, $n = 1, 2, \ldots$, *являются правосторонне симметричные* $(0,1)-$*матрицы* $\boldsymbol{J}_W$ $n-$*го порядка* (необходимые условия), *невырожденные над полем* F_2 (достаточные условия).

Определение. *Правосторонне симметричными будем называть квадратные матрицы произвольного порядка, симметричные относительно вспомогательной диагонали.*

Утверждение 2. *Индикаторные матрицы* $\boldsymbol{J}_W$ *систем функций Уолша* $\boldsymbol{W}$ $N-го$ *порядка однозначно определяют правило перестановки номеров отсчетов* t *дискретного сигнала* $x(t)$ *на входе процессора БПФ, формирующего дискретный спектр* $\boldsymbol{X}(k)$, $k=\overline{0, N-1}$, *в базисе* $\boldsymbol{W}$. *Правило перестановки задается соотношением* $t = l \cdot (\mathbf{1} \cdot \bar{\boldsymbol{J}}_W)$, $l=\overline{0, N-1}$, *где* $\mathbf{1}-$ *матрица инверсной перестановки, а* $\bar{\boldsymbol{J}}_W -$ *матрица, обратная ИМ.*

Существенно большего числа симметричных базисов можно достичь во множестве так называемых *Уолша-подобных систем секвентных функций*. В отличие от функций классических систем Уолша базисные Уолша-подобные секвентные функции двоично-степенного порядка совсем не обязательно должны содержать в пространстве оригиналов одинаковое число знаков +1 и –1 (или соответственно 0 и 1 в пространстве изображений) в их левой и правой половинках. Достаточными является такие условия: каждая секвентная функция в пространстве изображений должна начинаться с нуля и содержать одинаковое число знаков 0 и 1, при том, что базисная функция нулевого порядка состоит из одних нулей.

Приведем сравнение мощности множеств базисов классических систем Уолша $L_W(n)$ с мощностью множества Уолша-подобных систем секвентных функций $L_S(n)$. Если, для примера, $L_W(3)=28$, то $L_S(3)=840$. Отношение $\gamma = L_S(n)/L_W(n)$ значимо возрастает с увеличением n.

Считается, что «хорошему» базису должны быть присущи, по крайней мере, такие свойства: полнота, ортогональность, мультипликативность и симметричность матрицы преобразования. Для криптографических приложений (но не для общего спектрального анализа сигналов) симметричность Уолша-подобных базисов не является строго обязательным условием, поскольку БПФ-зашифрованное сообщение (изображение или видеосигнал) успешно расшифровывается тем же несимметричным базисом. Отмеченное обстоятельство приводит к тому, что криптостойкость алгоритмов БПФ-шифрования к лобовым атакам становится равным величине $N!/2$.

На основании проделанных исследований приходим к следующим основным результатам и выводам:

1. Решена задача синтеза полного множества систем функций Уолша и Уолша-подобных секвентных систем, используемых в качестве базисов БПФ-шифрования растровых изображений и видеосигналов.

2. Оказалось лишним решение задачи факторизации матриц классических и Уолша-подобных систем функций поскольку в алгоритмах БПФ в различных базисах структура дерева преобразования сохраняется неизменной и повторяет схему Кули-Тьюки, а смена базиса достигается элементарными перестановками номеров отсчетов сигнала на входе процессора БПФ.